PEJABAT SETIAUSAHA KERAJAAN PAHANG

POLISI KESELAMATAN SIBER VERSI 4.0

SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUATKUASA
15 September 2009	1.0	JPICT (15 September 2009)	15 September 2009
10 Oktober 2011	2.0	YB Setiausaha Kerajaan Pahang	10 Oktober 2011
18 April 2017	2.1	YB Setiausaha Kerajaan Pahang	18 April 2017
15 Julai 2020	2.2	YB Setiausaha Kerajaan Pahang	15 Julai 2020
26 Mac 2021	2.3	YB Setiausaha Kerajaan Pahang	23 Februari 2022
21 Dis 2022	3.0	YB Setiausaha Kerajaan Pahang	1 Februari 2023
31 Dis 2024	4.0	YB Setiausaha Kerajaan Pahang	15 Januari 2025

JADUAL PINDAAN POLISI KESELAMATAN SIBER
PEJABAT SETIAUSAHA KERAJAAN PAHANG

TARIKH	VERSI	BUTIRAN PINDAAN
10 Oktober 2011	2.0	i. Pindaan mengikut format ISO/IEC 17799:2005 dan juga format DKICT MAMPU ii. Tajuk baru: Penilaian Risiko Keselamatan ICT
18 April 2017	2.1	i. Pindaan mengikut Surat Kelulusan Perjawatan Baru Pejabat SUK Pahang Tahun 2016 ii. Terdapat beberapa perubahan nama lokasi beberapa kawasan larangan di Pejabat SUK Pahang selaras dengan penyusunan semula nama blok. iii. Pindaan turut mematuhi keperluan MS ISO/IEC 27001:2013 ISMS yang telah diperolehi Pejabat SUK Pahang pada tahun 2015. iv. Penambahan beberapa pekeliling dan surat arahan baru Pejabat SUK Pahang. v. Pindaan nama dokumen daripada 'Dasar Keselamatan ICT Pejabat SUK Pahang' kepada 'Polisi Keselamatan Siber Pejabat Setiausaha Kerajaan Pahang berdasarkan Rangka Kerja Keselamatan Sektor Awam (RAKKSSA) Versi 1.0 MAMPU bertarikh April 2016.
15 Julai 2020	2.2	i. Tambahan sub bidang bagi 020111 Pentadbir Storan Awan (*Cloud Storage).* ii. Tambahan sub bidang bagi 050205 Media Mudah Alih Persendirian (Bring Your Own Device). iii. Tambahan Sub bidang 0707 Kawalan Capaian Perkhidmatan *Hosting.* iv. Pembetulan ayat dan ejaan. v. Pindaan agensi berkaitan dari GCERT MAMPU kepada NACSA MKN dalam sub modul 020104.
26 Mac 2021	2.3	i. Pindaan polisi kata laluan di Bidang 07 Kawalan Capaian. ii. Pindaan jenis-jenis talian yang dibenarkan selain 1PahangNet di Bidang 0606.
21 Dis 2022	3.0	i. Perubahan polisi selaras dengan keperluan ISO/IEC 27001:2013 ISMS dan PKS MAMPU mengikut Arahan Pentadbiran Ketua Pengarah MAMPU bil.4 Tahun 2020.
31 Dis 2024	4.0	i. Perubahan polisi selaras dengan keperluan ISMS ISO/IEC 27001:2022. ii. Pindaan kandungan dari 14 bidang kepada 4 kategori selaras dengan keperluan ISMS ISO/IEC 27002:2022 iii. Pertambahan sebelas (11) kawalan baru selaras dengan keperluan ISMS versi 2022 adalah seperti berikut:

		a. Kawalan 5.7 Risikan Ancaman (*Threat Intelligence)* b. Kawalan 5.23 Keselamatan Maklumat Bagi Penggunaan Perkhidmatan Awan *(Information Security For Use Of Cloud Services)* c. Kawalan 5.30 Perkhidmatan (ICT Readiness for Business Continuity d. Kawalan 7.4 Pemantauan Keselamatan Fizikal (Physical Security Monitoring) e. Kawalan 8.9 Pengurusan Konfigurasi (Configuration Management) f. Kawalan 8.10 Penghapusan Maklumat (Information Deletion) g. Kawalan 8.11 Pelitupan Data (Data Masking) h. Kawalan 8.12 Pencegahan Kebocoran Data (Data Leakage Prevention) i. Kawalan 8.16 Aktiviti Pemantauan (Monitoring Activities) j. Kawalan 8.22 Pengasingan Rangkaian (Segregation Of Networks) k. Kawalan 8.28 Pengekodan Selamat (Secure Coding)

KANDUNGAN

TAKRIFAN

1.	Anti virus	Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, optical disk, flash disk, CDROM untuk sebarang kemungkinan adanya virus.
2.	Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
3.	Aset Alih	Aset yang boleh dipindahkan dari satu tempat ke satu tempat yang lain termasuk aset yang dibekalkan atau dipasang bersekali dengan bangunan.
4.	*Backup* (Sandaran)	Proses penduaan sesuatu dokumen atau maklumat
5.	Baki risiko	Risiko yang tinggal atau berbaki selepas pengolahan risiko dilaksanakan.
6.	*Bandwidth*	Lebar Jalur
7.	BCP/PKP	*Business Continuity Planning* / Pelan Kesinambungan Perkhidmatan
8.	*CCTV*	*Closed-Circuit Television System* Sistem TV yang digunakan secara komersil di mana satu sistem TV kamera video dipasang di dalam premis pejabat bagi tujuan membantu pemantauan fizikal.
9.	*CIA*	*Confidentiality, Integrity, Availability*
10.	*CDO*	*Chief Digital Officer* Ketua Pegawai Digital yang bertanggungjawab terhadap ICT dan maklumat digital bagi menyokong arah tuju sesebuah organisasi.
11.	*Clear Desk dan Clear Screen*	Tidak meninggalkan dokumen data dan maklumat dalam keadaan terdedah di atas meja atau di paparan skrin komputer apabila pengguna tidak berada di tempatnya.
12.	*Denial of service*	Halangan pemberian perkhidmatan
13.	*Defence-in-depth*	Merupakan satu pendekatan dalam keselamatan siber di mana merupakan satu mekanisme lapisan pertahanan untuk melindungi data dan maklumat.
14.	*Downloading*	Aktiviti muat turun sesuatu perisian.
15.	*Encryption*	Enkripsi atau penyulitan ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
16.	*Escrow (*eskrow)	Sebarang sistem yang membuat salinan kunci penyulitan supaya boleh dicapai oleh individu yang dibenarkan pada bila-bila masa.
17.	*Forgery*	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*) dan penipuan (*hoaxes*).
18.	CSIRT Pahang	*Cyber Security and Incident Response Teams* atau Pasukan Tindak Balas Keselamatan Siber Pejabat SUK Pahang.
19.	*Hard disk*	Cakera keras. Digunakan untuk menyimpan data dan boleh diakses lebih pantas.
20.	*Hub*	Hab merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan

		(broadcast) data yang diterima daripada sesuatu port kepada semua port yang lain.
21.	*ICT*	*Information and Communication Technology* Teknologi Maklumat dan Komunikasi
22.	*ICTSO*	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan siber.
23.	Impak teknikal	Melibatkan perkara-perkara yang menjejaskan kerahsiaan, integriti, ketersediaan dan akauntabiliti.
24.	BTM	Bahagian Teknologi Maklumat
25.	BKP	Bahagian Khidmat Pengurusan

TUJUAN

Polisi Keselamatan Siber Pejabat SUK Pahang ini bertujuan untuk menerangkan mengenai tanggungjawab dan peraturan-peraturan yang perlu difahami dan dipatuhi oleh kakitangan Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang dalam melindungi maklumat di ruang siber.

LATAR BELAKANG

Polisi ini dibangunkan untuk menjamin kesinambungan urusan Pejabat SUK Pahang dengan meminimumkan kesan insiden keselamatan siber. Polisi ini akan memudahkan perkongsian maklumat sesuai dengan keperluan operasi Pejabat SUK Pahang bagi memastikan semua maklumat dilindungi.

OBJEKTIF

Objektif utama Polisi Keselamatan Siber ini dibangunkan adalah seperti yang berikut:

a. Menerangkan kepada semua pengguna merangkumi warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang mengenai tanggungjawab dan peranan mereka dalam melindungi maklumat di ruang siber.

b. Memastikan keselamatan penyampaian perkhidmatan Pejabat SUK Pahang di tahap tertinggi sekali gus meningkatkan tahap keyakinan pihak berkepentingan seperti agensi Kerajaan, industri dan orang awam;

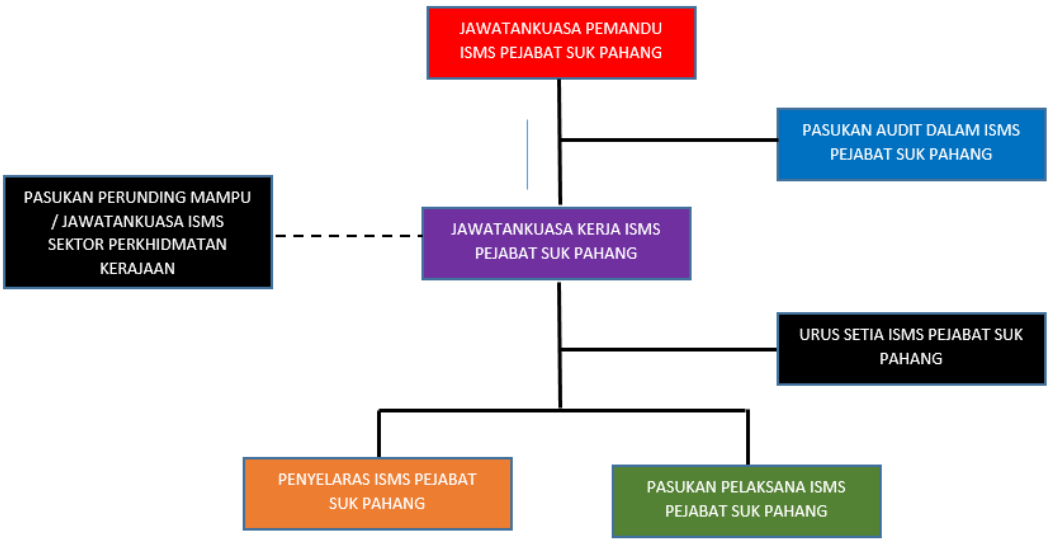
c. Memastikan kelancaran operasi Pejabat SUK Pahang dengan meminimumkan kerosakan atau kemusnahan disebabkan oleh insiden yang berlaku;

d. Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan yang berlaku dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan

e. Menyediakan ruang bagi penambahbaikan yang berterusan kepada pengurusan keselamatan dan pentadbiran ICT.

TADBIR URUS

Bagi memastikan keberkesanan dan kejayaan pelaksanaan PKS Pejabat SUK Pahang, satu (1) struktur tadbir urus iaitu Jawatankuasa Pemandu ISMS Pejabat Setiausaha Kerajaan Pejabat SUK Pahang telah diwujudkan seperti berikut:



Keahlian Jawatankuasa ini adalah seperti yang berikut:

Ketua: CDO (Timbalan Setiausaha Kerajaan Pahang (Pengurusan))

Ahli:

a. SUB BTM
b. SUB Bahagian-bahagian yang terlibat dengan skop ISMS
c. Pasukan Pelaksana ISMS
d. Pasukan Penyelaras ISMS
e. Urusetia ISMS

Peranan Jawatankuasa adalah berkaitan:

a. Pelaksanaan pensijilan ISMS ke atas perkhidmatan Pejabat Setiausaha Kerajaan Pahang yang dikenal pasti;

b. Kelulusan ke atas dasar, objektif dan skop pelaksanaan ISMS;

c. Penetapan kriteria penerimaan risiko, tahap risiko dan pelan penguraian risiko;

d. Keputusan dan tindakan Mesyuarat Jawatankuasa Kerja ISMS;

e. Kajian semula pelaksanaan pensijilan ISMS ke atas perkhidmatan-perkhidmatan Pejabat Setiausaha Kerajaan Pahang yang dikenal pasti;

f. Dasar dan objektif ISMS diwujudkan selaras dengan hala tuju strategik Pejabat Setiausaha Kerajaan Pahang;

g. Keperluan ISMS diterapkan dalam budaya kerja pegawai Pejabat Setiausaha Kerajaan Pahang;

h. Sumber yang diperlukan oleh pasukan pelaksana ISMS;

i. Kepentingan pengurusan ISMS yang berkesan dan pematuhan terhadap keperluannya;

j. Pencapaian sasaran ISMS seperti yang dirancang;

k. Arahan dan sokongan kepada Pasukan ISMS Pejabat Setiausaha Kerajaan Pahang bagi memastikan ISMS dapat dilaksanakan dengan berkesan; dan

l. Pelaksanaan program penambahbaikan dan peningkatan ISMS yang berterusan.

ASET ICT PEJABAT SETIAUSAHA KERAJAAN PAHANG

Polisi ini meliputi semua sumber atau aset ICT yang digunakan seperti :

a. Maklumat

i. Semua penyedia perkhidmatan dalam Pejabat SUK Pahang hendaklah mengenai pasti maklumat yang dijana dan hendaklah mengasingkannya mengikut kategori:

1. Maklumat Rahsia Rasmi - Di bawah Akta Rahsia Rasmi 1972 (Akta 88), maksud Maklumat Rahsia Rasmi ialah apa-apa suratan yang dinyatakan dalam Jadual kepada Akta Rahsia Rasmi 1972 (Akta 88) dan apa-apa maklumat dan bahan berhubungan dengannya dan termasuklah apa-apa dokumen rasmi, maklumat dan bahan Iain sebagaimana yang boleh dikelaskan sebagai "Rahsia Besar", "Rahsia", "Sulit" atau "Terhad" mengikut mana yang berkenaan oleh seorang Menteri, Menteri Besar atau Ketua Menteri sesuatu negeri atau mana-mana pegawai awam yang dilantikdi bawah seksyen 2B Akta Rahsia Rasmi 1972.

2. Maklumat Rasmi - maklumat yang diwujudkan, digunakan, diterima atau dikeluarkan secara rasmi oleh Pejabat SUK Pahang semasa menjalankan

urusan rasmi. Maklumat rasmi ini juga merupakan rekod awam yang tertakluk di bawah peraturan-peraturan Arkib Negara.

3. Maklumat Pengenalan Peribadi - Maklumat Pengenalan Peribadi (PII atau Personally Identifiable Information) ialah maklumat yang boleh digunakan secara tersendiri atau digunakan bersama maklumat lain untuk mengenai pasti individu tertentu. Data PII mengandungi data peribadi dan data sensitif individu. PII boleh juga terkandung dalam Maklumat Rahsia Rasmi.

4. Data Terbuka - Data terbuka merujuk kepada data kerajaan yang boleh digunakan secara bebas, boleh dikongsikan dan digunakan semula oleh rakyat, agensi sektor awam atau swasta untuk sebarang tujuan. PII dikecualikan daripada data terbuka.

b. Aliran Data

i. Aliran data merujuk kepada laluan lengkap data tertentu semasa transaksi. Aliran data dan komunikasi dalam Pejabat SUK Pahang hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Saluran komunikasi termasuk:

1. Saluran komunikasi dan aliran data antara sistem di Pejabat SUK Pahang;
2. Saluran komunikasi dan aliran data ke sistem luar; dan
   Saluran komunikasi dan aliran data ke ruang storan pengkomputeran awan dianggap sebagai saluran komunikasi luaran.

c. Platform Aplikasi dan Perisian

i. Semua platform aplikasi dan perisian hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala.

d. Peranti Fizikal dan Sistem

i. Semua peranti fizikal dan sistem hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Peranti fizikal termasuk:

1. Pelayan;
2. Peranti/Peralatan Rangkaian;
3. Komputer Peribadi/Komputer Riba;
4. Telefon/peranti pintar;
5. Media Storan;
6. Peranti dengan sambungan ke rangkaian, contohnya pengimbas, mesin pencetak, sistem kawalan akses, alat kawalan dan sistem kamera litar tertutup (CCTV);
7. Peranti pengkomputeran peribadi milik persendirian yang digunakan untuk urusan rasmi

Pejabat SUK Pahang; dan

8. Peranti pengesahan (authentication devices), contohnya token keselamatan, dongle dan alat pengimbas biometrik.

e. Sistem Luaran

i. Sistem luaran ialah sistem bukan milik Pejabat SUK Pahang yang dihubungkan dengan sistem Pejabat SUK Pahang. Semua sistem luaran hendaklah dikenal pasti, direkodkan dan dinilai tahap keselamatannya secara berkala.

f. Sumber Luaran

i. Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkod dan dinilai tahap keselamatannya secara berkala. Perkhidmatan sumber luaran ialah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi Pejabat SUK Pahang. Contoh perkhidmatan sumber luaran ialah:

1. Perisian Sebagai Satu Perkhidmatan
2. Platform Sebagai Satu Perkhidmatan
3. Infrastruktur Sebagai Satu Perkhidmatan
4. Storan Pengkomputeran Awan
5. Pemantauan Keselamatan

ii. Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan, dikaji semula dan dipastikan keselamatannya secara berkala.

Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran langkah-langkah keselamatan.

RISIKO

Pejabat SUK Pahang hendaklah mengenai pasti risiko yang berkaitan dengan maklumat yang terlibat. Risiko ialah kebarangkalian Pejabat SUK Pahang tidak dapat melaksanakan fungsi jabatan dengan baik. Penilaian risiko hendaklah dilaksanakan bagi menilai risiko terjejasnya kerahsiaan, integriti dan ketersediaan maklumat dalam ruang siber Pejabat SUK Pahang.

Penilaian risiko hendaklah dilaksanakan sekurang-kurangnya sekali setahun atau apabila berlaku sebarang perubahan kepada persekitaran siber Pejabat SUK Pahang .

Penilaian risiko hendaklah dikenal pasti dan dilaksanakan dengan tindakan berikut:

a. Kerentanan

Kerentanan adalah kelemahan atau kecacatan aset yang mungkin dieksploitasi dan mengakibatkan pelanggaran keselamatan. Kerentanan setiap aset hendaklah dikenal pasti sebagai sebahagian daripada proses pengurusan risiko.

b. Ancaman

Pejabat SUK Pahang hendaklah mengenai pasti ancaman yang disengajakan atau tidak disengajakan yang mungkin mengeksploitasi sebarang kelemahan yang telah dikenal pasti.

c. Impak

Pejabat SUK Pahang hendaklah menganggarkan impak insiden yang mungkin terjadi. Impak boleh dikategorikan kepada impak teknikal dan impak berkaitan dengan fungsi Pejabat SUK Pahang.

d. Tahap Risiko

Tahap risiko ditentukan daripada ancaman, kebarangkalian dan impak risiko. Kaedah penentuan hendaklah mengikut polisi penilaian atau pengurusan risiko yang sedang berkuat kuasa.

e. Penguraian Risiko

Penguraian risiko hendaklah dikenal pasti untuk menentukan sama ada risiko perlu dielakkan, dikurangkan, diterima atau dipindahkan dengan mengambil kira kos/faedahnya.

Ancaman berkaitan baki risiko dan risiko yang diterima hendaklah dipantau secara berkala dengan mengambil kira perkara berikut:

1. Teknologi

   Teknologi hendaklah dikenal pasti untuk mengurangkan risiko. Sebagai contoh, tembok api digunakan untuk mengehadkan capaian logikal kepada sistem tertentu.

2. Proses

   Perekayasaan proses, Prosedur Operasi Standard dan polisi hendaklah dikenal pasti untuk mengurangkan risiko.

3. Manusia

   Mengenai pasti sumber manusia berkelayakan dan kompeten yang mencukupi serta memastikan pengurusan sumber manusia dilaksanakan sebagai pengolahan risiko yang berkesan.

f. Pengurusan Risiko

1. Penyedia perkhidmatan digital di Pejabat SUK Pahang hendaklah memastikan tadbir urus pengurusan risiko diwujudkan dengan mengambil kira perkara berikut:
   i. mengenai pasti kerentanan;
   ii. mengenai pasti ancaman;
   iii. menilai risiko;
   iv. menentukan penguraian risiko;
   v. memantau keberkesanan penguraian risiko; dan
   vi. memantau ancaman yang berkaitan dengan baki risiko dan risiko yang diterima.

2. Tahap Risiko dan Pengurusan Risiko hendaklah dijadikan agenda tetap dan dibincangkan sekurang-kurangnya sekali setahun oleh JKK ISMS dan dimaklumkan kepada Mesyuarat Jawatankuasa Pemandu ISMS Pejabat SUK Pahang.

PRINSIP KESELAMATAN

Prinsip-prinsip yang menjadi asas kepada Polisi Keselamatan Siber Pejabat SUK Pahang dan perlu dipatuhi adalah seperti berikut:

a. Prinsip “Perlu-Tahu”

Pejabat SUK Pahang hendaklah melaksanakan mekanisme bagi memberikan kebenaran kepada capaian maklumat. Maklumat yang dicapai oleh pengguna yang dibenarkan hendaklah berdasarkan prinsip “Perlu-Tahu” yang membenarkan capaian maklumat yang diperlukan untuk melaksanakan tugasnya sahaja.

Bagi capaian spesifik Maklumat Rahsia Rasmi, penggunaan yang dibenarkan hendaklah dihadkankepada masa, lokasi, peranan dan fungsi pengguna tersebut.

b. Hak Keistimewaan minimum

Pengguna hendaklah diberikan hak keistimewaan minimum iaitu terhad kepada keperluan untuk menjalankan tugasnya. Hak akses pengguna hanya diberi pada tahap yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Prinsip ini digunakan untuk menyekat hak akses kepada aplikasi, sistem, proses dan peranti kepada pengguna yang dibenarkan untuk melaksanakan aktiviti. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas.

c. Pengasingan Tugas

Bagi mengekalkan prinsip sekat-dan-imbang (check and balance), Pejabat SUK Pahang hendaklah melaksanakan pengasingan tugas bagi tugas yang kritikal supaya tidak dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya.

d. Kawalan Capaian Berdasarkan Peranan

Capaian sistem hendaklah dihadkan kepada pengguna yang dibenarkan mengikut peranan dalam fungsi tugas mereka dan kebenaran untuk melaksanakan operasi tertentu adalah berdasarkan peranan tersebut.

e. Peminimuman Data

Pejabat SUK Pahang hendaklah mengamalkan prinsip peminimuman data yang mengehadkan penyimpanan data peribadi kepada yang diperlukan dan disimpan dalam tempoh yang diperlukan sahaja.

TEKNOLOGI

Teknologi untuk melindungi data hendaklah dikenal pasti di semua peringkat pemprosesan data di setiap elemen pengkomputeran seperti berikut:

a. Peringkat Pemprosesan Data

1. Data-dalam-simpanan

   i. Pejabat SUK Pahang hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-simpanan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data-dalam-simpanan.

   ii. Maklumat Rahsia Rasmi, Maklumat Rasmi dan PII perlu dilindungi daripada segi kerahsiaan dan integriti data. Data terbuka perlu dilindungi daripada segi integriti data.

2. Data-dalam-pergerakan

   Pejabat SUK Pahang hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-pergerakan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data-dalam-pergerakan.

3. Data-dalam-penggunaan

   i. Pejabat SUK Pahang hendaklah menggunakan teknologi yang bersesuaian untuk melindungi data-dalam-penggunaan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Di samping itu, teknologi untuk menentukan asal data dan tanpa sangkalan mungkin diperlukan. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data dalam penggunaan.

   ii. Teknologi yang bersesuaian boleh digunakan untuk memastikan keaslian data dan data/transaksi tanpa-sangkal.

4. Perlindungan Ketirisan Data

   i. Teknologi perlindungan ketirisan data bertujuan untuk menghalang pengguna yang sah daripada menyebarkan maklumat tanpa kebenaran.

   ii. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk menghalang atau mengesan ketirisan data.

b. Elemen Dalam Persekitaran Pengkomputeran

Berdasarkan penilaian risiko dan pelan pengurusan risiko, Pejabat SUK Pahang hendaklah menggunakan kaedah teknologi dan kawalan keselamatan (*countermeasure and control measure*) yang dapat melindungi data di semua peringkat saluran pemprosesan bagi semua elemen dalam persekitaran pengkomputeran.

Maklumat Terkawal (Rahsia Rasmi) hendaklah disimpan dan diproses dalam persekitaran penghomputeran mengikut Prosedur Kawalan Keselamatan Dokumen Pejabat SUK Pahang yang dikeluarkan oleh Pejabat SUK Pahang.

Setiap projek ICT yang dibangunkan di Pejabat SUK Pahang dan menyimpan maklumat terkawal hendaklah mempunyai Pelan Pengurusan Keselamatan Maklumat tersendiri yang mengandungi maklumat terperinci berhubung seni bina sistem, teknologi dan kawalan keselamatan bagi setiap kategori elemen di bawah:

1. Peranti pengkomputeran peribadi

    i. Peranti pengkomputeran peribadi merujuk kepada peranti komputer yang digunakan oleh manusia untuk berinteraksi dengan sistem. Contoh peranti pengkomputeran peribadi ialah komputer riba, stesen kerja dan peranti storan.
    ii. Pengguna yang menggunakan peranti pengkomputeran peribadi milik persendirian untuk mencapai Maklumat Terkawal hendaklah memohon kebenaran daripada pihak bertanggungjawab di Pejabat SUK Pahang.

2. Peranti rangkaian

    i. merujuk kepada peranti yang digunakan untuk membolehkan saling hubungantara peranti komputer dan sistem seperti suis, penghala, tembok api, peranti VPN dan kabel.
    ii. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-pergerakan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

3. Aplikasi

    i. Perisian aplikasi digunakan oleh manusia untuk memproses dan berinteraksi dengan data. Contoh perisian aplikasi ialah pelayan web, pelayan aplikasi, sistem operasi.
    ii. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

4. Pelayan

   i. Pelayan merujuk kepada peranti pengkomputeran yang mengandungi aplikasi dan storan. Pelayan hendaklah diletakkan di lokasi yang selamat.
   ii. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

5. Persekitaran fizikal

   i. Persekitaran fizikal merujuk kepada lokasi fizikal yang menempatkan sistem ICT.
   ii. Pejabat SUK Pahang hendaklah merujuk kepada Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia untuk mendapatkan nasihat mengenai cadangan yang berkaitan dengan pengambilalihan, pajakan, pengubahsuaian, pembelian bangunan milik Kerajaan dan swasta yang menempatkan kemudahan pemprosesan maklumat.
   iii. Perlindungan fizikal yang disediakan hendaklah selaras dengan risiko yang dikenal pasti dan berdasarkan prinsip *defence-in-depth*.
   iv. Teknologi dan kawalan keselamatan yang dikenal pasti untuk melindungi data-dalam-penggunaan, data-dalam-pergerakan, data-dalam-simpanan dan menghalang ketirisan data hendaklah diperincikan dalam Pelan Pengurusan Keselamatan Maklumat.

PROSES

Warga Pejabat SUK Pahang hendaklah melindungi keselamatan siber dengan melaksanakan perkara-perkara berikut:

a. Konfigurasi Asas

1. Semua sistem hendaklah mempunyai satu konfigurasi asas yang direkodkan dan menjadi prasyarat pentauliahan sistem.
2. Konfigurasi asas yang baharu hendaklah diwujudkan selaras dengan prosedur kawalan perubahan.

b. Kawalan Perubahan Konfigurasi

1. Prosedur kawalan perubahan konfigurasi hendaklah diwujud dan dilaksana bagi perubahan kepada sistem, termasuk tampalan perisian, pakej perkhidmatan, konfigurasi rangkaian dan pengemaskinian sistem operasi.
2. Sebarang perubahan yang tidak termasuk dalam konfigurasi asas hendaklah diluluskan oleh jawatankuasa yang dilantik atau diberi kuasa berdasarkan prosedur kawalan perubahan konfigurasi bagi menghasilkan konfigurasi asas terkini.
3. Jawatankuasa yang dilantik atau diberi kuasa hendaklah menentukan keperluan untuk melaksanakan Penilaian Tahap Keselamatan berdasarkan jangkaan impak perubahan.

c. Sandaran

1. Sandaran hendaklah dilaksanakan secara berkala berdasarkan peraturan semasa yang sedang berkuat kuasa untuk memastikan bahawa sistem boleh dipulihkan.
2. Media sandaran hendaklah disimpan dalam persekitaran yang selamat dan di lokasi yang berasingan.

d. Kitaran Pengurusan Aset

1. Pindah

i. Pemindahan hak milik aset berlaku dalam keadaan berikut:

a) Warga Pejabat SUK Pahang meninggalkan agensi disebabkan oleh persaraan, perletakan jawatan atau penugasan semula;

b) Aset yang dikongsi untuk kegunaan sementara;

c) Pemberian aset kepada agensi lain; dan

d) Aset dikembalikan setelah tamat tempoh sewaan.

ii. Data dalam peranti tersebut hendaklah diuruskan mengikut tatacara pelupusan di perkara (2).

2. Pelupusan

i. Pelupusan media storan hendaklah dirujuk kepada CGSO sebagai langkah pertama di mana CGSO akan membuat keputusan sama ada sistem itu mengandungi maklumat terperingkat atau sebaliknya.

ii. Berdasarkan keputusan CGSO, pelupusan perlu dirujuk kepada Arkib Negara Malaysia bagi semakan sama ada sistem itu mengandungi maklumat yang termaktub di bawah tindakan Akta Arkib Negara 2003 (Akta 629) dan Warta Kerajaan P.U.(A)377. Peraturan-Peraturan Arkib Negara (Penetapan Borang-Borang bagi Pelupusan Rekod Awam) 2008.

iii. Pelupusan boleh dalam bentuk pemusnahan fizikal dan/atau sanitasi data.

iv. Sanitasi data hendaklah mengikut Garis Panduan Sanitasi Media Elektronik Sektor Awam yang sedang berkuat kuasa.

3. Kitaran Hayat

i. Kitaran hayat data hendaklah diuruskan mengikut Akta 629.

ii. Akta 629 memberikan mandat bahawa rekod kewangan hendaklah disimpan selama tujuh tahun dan rekod umum selama lima tahun.

MANUSIA

Warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak-pihak yang berkepentingan hendaklah memahami peranan dan tanggungjawab mereka. Mereka hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuatkuasa.

Sistem penyampaian perkhidmatan Kerajaan hendaklah dikendalikan oleh individu yang kompeten dan berpengetahuan. Kakitangan hendaklah dilatih dalam bidang pengkhususan yang diperlukan. Asas kecekapan pengguna hendaklah dibangunkan bagi semua warga Pejabat SUK Pahang.

a. Kompetensi pengguna

1. Kompetensi pengguna termasuk:

i. Kesedaran amalan terbaik keselamatan maklumat dengan memupuk amalan baik keselamatan siber dengan mewujudkan komunikasi ICT dan program kesedaran keselamatan siber.

ii. Kemahiran menggunakan alat keselamatan dengan menyediakan latihan yang mencukupi kepada warga Pejabat SUK Pahang berhubung alat-alat keselamatan berkaitan untuk memastikan mereka mampu untuk melaksanakan tugas harian mereka.

iii. Kompetensi pengguna hendaklah tertakluk kepada penilaian berkala melalui ujian khusus.

iv. Setiap orang yang diberi kuasa untuk mengendalikan dokumen terperingkat, kompetensi tambahan pengguna selaras dengan arahan/pekeliling semasa adalah diharapkan.

b. Kompetensi pelaksana

1. Warga Pejabat SUK Pahang yang menguruskan aset ICT hendaklah memenuhi keperluan kecekapan minimum mengikut spesifikasi kerja mereka.

2. Pegawai Keselamatan ICT hendaklah memenuhi syarat-syarat berikut:

i. Mempunyai kelayakan akademik dalam bidang berkaitan atau sijil profesional keselamatan siber.

ii. Memenuhi keperluan pembelajaran berterusan.

iii. Menimba pengalaman yang mencukupi dalam bidang keselamatansiber.

iv. Memperolehi tapisan keselamatan daripada agensi yang diberikuasa.

3. Pegawai Keselamatan ICT yang dilantik hendaklah memenuhi keperluan kompetensi di atas. Pegawai Keselamatan ICT bertanggungjawab untuk merancang, mengurus dan melaksanakan program keselamatan di Pejabat SUK Pahang.

c. Peranan

1. Peranan pengguna hendaklah diberi berdasarkan keperluan dan kompetensi pengguna.
2. Tiada hak capaian automatik diberikan kepada individu tanpa mengira tapisan keselamatan mereka.
3. Warga Pejabat SUK Pahang yang berperanan menguruskan aset ICT hendaklah memastikan semua aset ICT Jabatan dikembalikan sekiranya berlaku perubahan peranan.
4. Warga Pejabat SUK Pahang yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Jabatan yang berkaitan seperti tersenarai dalam senarai aset dalam Nota Serah Tugas.
5. Warga Pejabat SUK Pahang yang terlibat dengan perubahan peranan hendaklah menyerahkan semua aset Jabatan dengan diselia oleh kakitangan yang dipertanggungjawabkan oleh Jabatan

PELAN PENGURUSAN KESELAMATAN MAKLUMAT

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan adalah suatu proses yang berterusan dan melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan siber sentiasa berubah.

Pernyataan ini merangkumi perlindungan semua bentuk maklumat elektronik dan bukan elektronik yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan yang dibuat salinan bagi memelihara keselamatan ruang siber dan ketersediaan maklumat kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

a. Kerahsiaan

   Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran.

b. Integriti

   Data dan maklumat hendaklah tepat, lengkap dan kemas kini dan hanya boleh diubah dengan cara yang dibenarkan.

c. Tidak Boleh Disangkal

   Punca data dan maklumat hendaklah daripada punca yang sah dan tidak boleh disangkal.

d. Kesahihan

   Data dan maklumat hendaklah dipastikan kesahihannya.

e. Ketersediaan

   Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain itu, langkah-langkah ke arah memelihara keselamatan siber hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan ICT Pejabat SUK Pahang, ancaman yang wujud akibat daripada kelemahan tersebut, risiko yang mungkin timbul dan langkah- langkah pencegahan yang perlu diambil untuk menangani risiko berkenaan.

Empat (4) kawalan yang terlibat di dalam Polisi Keselamatan Siber Pejabat SUK Pahang diterangkan dengan lebih jelas dan teratur dalam dokumen ini.

A.1 KAWALAN POLISI KESELAMATAN MAKLUMAT (*INFORMATION SECURITY POLICY CONTROLS*)	
5.0 KAWALAN ORGANISASI (*ORGANIZATIONAL CONTROL*)	
5.1 POLISI KESELAMATAN MAKLUMAT (POLICIES FOR INFORMATION SECURITY)	**PERANAN**
1) Pelaksanaan Polisi ini akan dijalankan oleh Pejabat SUK Pahang dengan disokong oleh Jawatankuasa ISMS terdiri daripada: i) Pengerusi ISMS ii) Pegawai Keselamatan ICT (ICTSO) iii) Ketua-ketua Bahagian iv) Ahli-ahli yang dilantik oleh Pejabat SUK Pahang Polisi ini perlu disebarkan dan dipatuhi oleh semua warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang. Satu set polisi untuk keselamatan maklumat perlu ditakrifkan, diluluskan, diterbitkan dan dimaklumkan oleh pihak Pengurusan Tertinggi Pejabat SUK Pahang kepada warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang.	Pihak Pengurusan Tertinggi Pejabat SUK Pahang
2) Polisi Keselamatan Siber ini adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, polisi kerajaan dan kepentingan sosial. Berikut adalah prosedur yang berkaitan dengan kajian semula Polisi Keselamatan Siber Pejabat SUK Pahang: a. Kenal pasti dan tentukan perubahan yang diperlukan; b. Kemuka cadangan pindaan secara bertulis untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Pemandu ICT Negeri Pahang (JPICT) / Setiausaha Kerajaan Pahang bagi tujuan pengesahan; c. Maklum kepada semua warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang berkenaan pindaan yang telah diluluskan; dan Polisi ini hendaklah dikaji semula **sekurang-kurangnya LIMA (5) tahun sekali** atau mengikut keperluan semasa bagi memastikan dokumen sentiasa relevan.	JPICT/CDO/ICTSO

5.2 PERANAN DAN TANGGUNGJAWAB KESELAMATAN MAKLUMAT *(INFORMATION SECURITY ROLES AND RESPONSIBILITIES)*	**PERANAN**
5.2.1 Peranan dan tanggungjawab Setiausaha Kerajaan Pahang adalah seperti berikut: a. Memastikan penguatkuasaan pelaksanaan Polisi ini; b. Memastikan semua warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang memahami dan mematuhi peruntukan-peruntukan di bawah Polisi ini; c. Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi; dan d. Memastikan pengurusan risiko dan program keselamatan siber dilaksanakan seperti yang ditetapkan di dalam Polisi ini; dan e. Melantik CDO dan ICTSO.	Setiausaha Kerajaan Pahang
5.2.2 Timbalan Setiausaha kerajaan Pahang (Pengurusan) adalah merupakan Ketua Pegawai Digital (CDO). Peranan dan tanggungjawab beliau adalah seperti berikut: a. Membantu Setiausaha Kerajaan Pahang dalam melaksanakan tugas-tugas yang melibatkan keselamatan siber seperti yang ditetapkan dalam Polisi ini; b. Memastikan kawalan keselamatan maklumat dalam Pejabat SUK Pahang diseragam dan diselaras dengan sebaiknya; c. Memastikan Pelan Strategik Pendigitalan Pejabat SUK Pahang mengandungi aspek keselamatan siber; dan d. Menyelaras pelan latihan dan program kesedaran keselamatan siber.	Ketua Pegawai Digital (CDO)
5.2.3 Setiausaha Bahagian Teknologi Maklumat (BTM) adalah merupakan ICTSO Pejabat SUK Pahang. Peranan dan tanggungjawab ICTSO adalah seperti berikut : a. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Polisi ini; b. Merangka pengurusan risiko dan audit keselamatan siber berpandukan rangka kerja, polisi, pekeliling/garis panduan, dan pelan pengurusan keselamatan maklumat yang berkuat kuasa; c. Menyedia dan menyebarkan amaran-amaran yang sesuai	Pegawai Keselamatan ICTSO

terhadap kemungkinan berlakunya ancaman keselamatan siber dan memberikan khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; d. Melaporkan insiden keselamatan siber kepada Agensi Keselamatan Siber Negara (NACSA), Majlis Keselamatan Negara dan seterusnya membantu dalam penyiasatan atau pemulihan. e. Melaporkan insiden kepada CDO bagi insiden yang memerlukan Pengurusan Kesinambungan Perkhidmatan (PKP); f. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan siber dan memperakukan langkah-langkah baik pulih dengan segera; g. Melaksanakan pematuhan Polisi ini oleh warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang; h. Menyemak, mengkaji dan menyediakan laporan berkaitan dengan isu-isu keselamatan siber; dan i. Menyedia dan merangka latihan dan program kesedaran keselamatan siber. j. Menjadi Pengarah Pasukan CSIRT Pejabat SUK Pahang.	Pegawai Keselamatan ICTSO
5.2.4 Semua Setiausaha Bahagian/Ketua Unit di Pejabat SUK Pahang berperanan dan bertanggungjawab dalam melaksanakan keperluan Polisi ini dalam operasi semasa bahagian/unit seperti yang berikut: a. Pelaksanaan sistem atau aplikasi baharu sama ada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baharu; b. Pembelian atau peningkatan perisian dan sistem komputer; c. Perolehan teknologi dan perkhidmatan komunikasi baru; d. Menentukan pembekal dan rakan usaha sama menjalani tapisan keselamatan; dan e. Memastikan pematuhan kepada pelaksanaan rangka kerja, polisi, pekeliling/garis panduan, dan pelan pengurusan keselamatan maklumat kerajaan yang berkuat kuasa.	Setiausaha Bahagian/Ketua Unit

5.2.5 Peranan dan tanggungjawab Pentadbir Sistem Aplikasi/Perkhidmatan Digital adalah seperti berikut: a. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; b. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Polisi ini; c. Memantau aktiviti capaian sistem aplikasi; d. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; e. Menganalisis dan menyimpan rekod jejak audit; f. Menyediakan laporan mengenai aktiviti capaian secara berkala; g. Memastikan kelancaran operasi sistem aplikasi supaya perkhidmatan yang disediakan tidak terjejas; h. Memastikan kod-kod program sistem aplikasi adalah selamat daripada penggodam sebelum sistem tersebut diaktifkan penggunaanya; i. Memastikan *hotfix* dan *patch* yang berkaitan dengan sistem aplikasi dikemaskini supaya terhindar daripada ancaman virus dan penggodam; j. Mematuhi dan melaksanakan prinsip-prinsip Polisi ini dalam pengujudan akaun pengguna ke atas setiap sistem aplikasi; k. Memastikan backup sistem aplikasi dan data yang berkaitan dengannya dibuat secara berjadual; l. Menghadkan capaian Dokumentasi Sistem Aplikasi bagi mengelakkan dari penyalahgunaannya; m. Melaporkan kepada CSIRT Pahang jika berlakunya insiden keselamatan ke atas sistem aplikasi di bawah pentadbirannya;	Pentadbir Sistem Aplikasi/Perkhidmatan Digital

5.2.6 Peranan dan tanggungjawab Pentadbir Teknikal adalah seperti berikut : a. Menyediakan khidmat sokongan teknikal ICT; b. Merancang dan melaksanakan perolehan aset ICT; c. Mengurus pendaftaran, agihan, penempatan dan pelupusan Aset ICT; d. Memastikan semua aset ICT diselenggarakan secara berkala dengan sempurna; e. Memastikan perisian antivirus dipasang pada Aset ICT; dan f. Mengurus Meja Bantuan ICT Pejabat SUK Pahang.	Pentadbir Teknikal
5.2.7 Peranan dan tanggungjawab Pentadbir Rangkaian adalah seperti berikut : a. Memastikan rangkaian setempat (LAN), rangkaian luas (WAN) dan rangkaian Pejabat SUK Pahang beroperasi sepanjang masa; b. Memastikan semua peralatan dan perisian rangkaian diselenggarakan dengan sempurna; c. Merancang peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada; d. Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidakstabil dan sebarang kerosakan perkakasan sokongan rangkaian Pejabat SUK Pahang; e. Memantau penggunaan rangkaian dan melaporkan kepada CSIRT Pejabat SUK Pahang sekiranya berlaku penyalahgunaan sumber rangkaian; f. Mewartakan polisi dan garis panduan penggunaan rangkaian Pejabat SUK Pahang kepada pengguna rangkaian; g. Memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan luar ke dalam rangkaian Pejabat SUK Pahang secara tidak sah; dan h. Menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian.	Pentadbir Rangkaian

5.2.8 Peranan dan tanggungjawab pentadbir Laman Web adalah seperti berikut: a. Menerima kandungan laman web yang telah disahkan kesahihan dan terkini daripada sumber yang sah; b. Memantau prestasi capaian dan menjalankan penalaan prestasi untuk memastikan akses yang lancar; c. Memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai muka laman; d. Menghadkan capaian Pentadbir Laman Web bahagian/unit ke web server; e. Memastikan reka bentuk web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; f. Melaporkan sebarang pelanggaran keselamatan laman portal kepada CSIRT Pejabat SUK Pahang.	Pentadbir Laman Web/portal (WEBMASTER)
5.2.9 Peranan dan tanggungjawab pentadbir E-Mel adalah seperti berikut: a. Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan Ketua Jabatan. Pembatalan akaun (pengguna yang berhenti, bertukar dan melanggar Polisi dan tatacara jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat; b. Pentadbir e-mel boleh membekukan akaun pengguna jika perlu semasa pengguna bercuti panjang, berkursus atau menghadapi tindakan tatatertib; c. Menyimpan jejak audit selama sekurang-kurangnya enam (1) bulan di dalam pelayan e-mel ATAU tertakluk kepada kemampuan ruang storan; d. Melaksanakan jadual penstoran dan pengarkiban e-mel. Penyimpanan media storan sama ada di luar atau di dalam kawasan mestilah mempunyai ciri-ciri keselamatan fizikal yang terjamin bagi mengelak daripada sebarang risiko seperti kehilangan maklumat; e. Memastikan akaun e-mel pengguna sentiasa dalam keadaan baik dan berfungsi; f. Memastikan keselamatan akaun e-mel pengguna dari ancaman luar dan dalam;	Pentadbir E-Mel

g. Melaksanakan penyelenggaraan ke atas sistem e-mel dengan baik dan menentukan segala *patches* terkini yang disediakan oleh pihak pembekal dipasang dan berfungsi dengan sempurna; h. Memantau status storan e-mel Pengurusan Atasan Pejabat SUK Pahang dan memastikan emel Pengurusan Atasan Pejabat SUK Pahang sentiasa tersedia untuk transaksi e-mel; i. Memastikan semua peralatan sistem e-mel sentiasa aktif 24 x 7; j. Memastikan agar keupayaan mail relay hanya boleh digunakan untuk server atau aplikasi dalaman Pejabat SUK Pahang sahaja bagi tujuan keselamatan; k. Memastikan kemudahan membuat capaian e-mel melalui pelbagai media seperti telefon mudah alih disediakan kepada pengguna e-mel Pejabat SUK Pahang; dan l. Memastikan pengguna e-mel Pejabat SUK Pahang berkemahiran menggunakan e-mel melalui penyediaan dokumen tatacara penggunaan e-mel Pejabat SUK Pahang dan Internet serta pelaksanaan Kursus Pembudayaan ICT (Penggunaan E-mel dan Internet) secara berterusan melalui latihan serta promosi.	Pentadbir E-Mel
5.2.10 Peranan dan tanggungjawab pegawai aset ICT adalah seperti berikut : a. Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya dalam keadaan yang baik; b. Memastikan Aset ICT milik Pejabat SUK Pahang dilabel dan direkodkan ke dalam Sistem Pengurusan Aset; c. Memastikan Aset milik Pejabat SUK Pahang dibuat pemeriksaan berkala secara tahunan dan diselenggara sebaiknya agar dapat meningkatkan jangka hayat Aset ICT tersebut; d. Memastikan Aset ICT untuk pinjaman dan simpanan sebelum agihan diletakkan di dalam bilik stor yang mempunyai kawalan keselamatan yang terjamin; e. Memastikan Stok alat ganti Aset ICT sentiasa mencukupi dan disimpan di tempat yang selamat dan terkawal; dan f. Memastikan Aset ICT yang ingin dilupuskan dilaksanakan	Pegawai Aset ICT

mengikut garis panduan kawalan keselamatan bagi pelupusan data digital.	
5.2.11 Peranan dan tanggungjawab pegawai adalah seperti berikut : a. Memastikan operasi Pusat Data dan DRC berada dalam keadaan baik 24 x 7; b. Merancang dan menyelia pelaksanaan simulasi *Disaster Recovery Plan* (DRP) Pejabat SUK Pahang; c. Mengurus operasi DRC sekiranya berlaku bencana terhadap Pusat Data Pejabat SUK Pahang; d. Memastikan operasi Infrastruktur Virtualisasi di Pusat Data dan DRC berfungsi dan diselenggara dengan baik bagi meningkatkan jangka hayat perkhidmatan perkakasan serta perisian; e. Memastikan operasi *backup / restore* data berfungsi dan diselenggara dengan baik bagi meningkatkan jangka hayat perkhidmatan perkakasan serta perisian; f. Memantau aset ICT sokongan dan fasiliti sokongan (Precision Aircond, Alat Pencegah Kebakaran, Alarm, Bekalan Elektrik) di Pusat Data dan DRC bagi memastikan beroperasi lancar 24 x 7; g. Menguruskan permohonan baru dan pengemaskinian server dan Virtual Machine bagi sistem aplikasi baru di Pusat Data dan DRC; h. Melaksanakan *housekeeping* keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di web server; dan pusat data; dan i. Menguruskan khidmat sokongan operasi server dari segi penerimaan, penyediaan, penyelenggaraan, waranti, pengeluaran dan pelupusan.	Pentadbir Pusat Data dan Disaster Recovery Center (DRC)
5.2.12 Peranan dan tanggungjawab Jawatankuasa ISMS adalah seperti berikut: a. Menentukan hala tuju keseluruhan pelaksanaan pensijilan ISMS Pejabat SUK Pahang yang merangkumi perancangan, pemantauan dan pengesahan terhadap perkara-perkara berikut: i. Pelaksanaan pensijilan ISMS ke atas perkhidmatan Pejabat SUK Pahang yangdikenalpasti;	Jawatankuasa Pemandu ISMS

ii. Kelulusan ke atas dasar, objektif, dan skop pelaksanaan ISMS; dan iii. Penetapan kriteria penerimaan risiko, tahap risiko dan *risk treatment plan.* b. Keputusan dan tindakan Mesyuarat Jawatankuasa Kerja ISMS Pejabat SUK Pahang; c. Kajian semula pelaksanaan pensijilan ISMS ke atas perkhidmatan-perkhidmatan Pejabat SUK Pahang yang dikenal pasti; d. Dasar dan objektif ISMS diwujudkan selaras dengan hala tuju strategik Pejabat SUK Pahang; e. Keperluan ISMS diterapkan dalam budaya kerja warga kerja Pejabat SUK Pahang; f. Sumber yang diperlukan oleh pasukan pelaksana ISMS; g. Kepentingan pengurusan ISMS yang berkesan dan pematuhan terhadap keperluannya; h. Pencapaian sasaran ISMS seperti yang dirancang; i. Arahan dan sokongan kepada pasukan ISMS Pejabat SUK Pahang bagi memastikan ISMS dapat dilaksanakan dengan berkesan; dan j. Pelaksanaan program penambahbaikan dan peningkatan ISMS yang berterusan. Meluluskan: a. Struktur Organisasi ISMS Pejabat SUK Pahang; b. Keperluan sumber; dan c. Pelantikan Pasukan Audit Dalam ISMS Pejabat SUK Pahang.	Jawatankuasa Pemandu ISMS
5.2.13 Peranan dan Tanggungjawab CSIRT adalah seperti berikut : a. Menerima dan mengesan aduan keselamatan siber dan menilai tahap dan jenis insiden; b. Merekodkan dan menjalankan siasatan awal insiden yang diterima;	Pasukan CSIRT Pejabat SUK Pahang

c. Menangani tindak balas (*response*) insiden keselamatan siber dan mengambil tindakan baikpulih minima; d. Menghubungi dan melaporkan insiden yang berlaku kepada NACSA MKN sama ada sebagai input atau untuk tindakan seterusnya; e. Menasihatkan agensi-agensi di bawah kawalannya mengambil tindakan pemulihan dan pengukuhan; f. Menyebarkan makluman berkaitan pengukuhan keselamatan siber kepada agensi di bawah kawalannya; dan g. Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	Pasukan CSIRT Pejabat SUK Pahang
5.2.14 Peranan dan tanggungjawab pengguna adalah seperti berikut: a. Membaca, memahami dan mematuhi Polisi ini; b. Mengetahui dan memahami implikasi keselamatan siber kesan dari tindakannya; c. Menjalani tapisan keselamatan sekiranya diperlukan dikehendaki berurusan dengan maklumatrasmi terperingkat; d. Mematuhi prinsip-prinsip Polisi ini dan menjaga kerahsiaan maklumat Pejabat SUK Pahang; e. Melaksanakan langkah-langkah perlindungan seperti berikut: i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan; iv. Menjaga kerahsiaan kata laluan; v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan siber yangditetapkan; vi. Melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukarandan pemusnahan; dan vii. Menjaga kerahsiaan bagi setiap langkah-langkah	Pengguna

keselamatan siber dari diketahuiumum. f. Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada Pasukan CSIRT Pejabat SUK Pahang dengan segera; g. Menghadiri program-program kesedaran mengenai keselamatan siber ; dan h. Menandatangani surat akuan pematuhan Polisi Keselamatan Siber Pejabat SUK Pahang di Sistem AkuanPKS Pejabat SUK Pahang di https://akuanpks.pahang.gov.my/ dan mencetak Surat Akuan yang dijana sebagaimana di **Lampiran 1.**	Pengguna
5.3 PENGASINGAN TUGAS *(SEGREGATION OF DUTIES)*	**PERANAN**
Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan peluang mengubah suai, tanpa kebenaran atau dengan tidak sengaja mengubah atau menyalah guna aset. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a. Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlakunya penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; b. Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; c. Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian; dan d. Pengasingan tugas bagi tugas yang kritikal tidak boleh dilaksanakan oleh seorang pengguna sahaja yang bertindak atas kuasa tunggalnya;	Setiausaha Bahagian/Ketua Unit

5.4 TANGGUNGJAWAB PENGURUSAN *(MANAGEMENT RESPONSIBILITIES)*	**PERANAN**
Pengurusan hendaklah memastikan warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang supaya mengamalkan keselamatan maklumat menurut polisi dan prosedur yang telah ditetapkan.	Warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang.
5.5 HUBUNGAN DENGAN PIHAK BERKUASA *(CONTACT WITH AUTHORITIES)*	**PERANAN**
Hubungan yang baik dengan pihak berkuasa berkaitan hendaklah dikekalkan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a. Hendaklah mengenal pasti perundangan dan peraturan yang berkaitan dalam melaksanakan peranan dan tanggungjawab Pejabat SUK Pahang; b. Mewujud dan mengemas kini prosedur/senarai pihak berkuasa perundangan/pihak yang dihubungi semasa kecemasan. Pihak berkuasa perundangan ialah Polis Diraja Malaysia dan Suruhanjaya Komunikasi Dan Multimedia. Pihak yang dihubungi semasa kecemasan termasuk juga pihak utiliti, pembekal perkhidmatan, perkhidmatan kecemasan, pembekal elektrik, keselamatan dan kesihatan serta bomba; dan c. Insiden keselamatan maklumat harus dilaporkan tepat pada masanya bagi mengurangkan impak insiden.	Pasukan ERT Dan CSIRT Pejabat Suk Pahang
5.6 HUBUNGAN DENGAN KUMPULAN BERKEPENTINGAN YANG KHUSUS *(CONTACT WITH SPECIAL INTEREST GROUPS)*	**PERANAN**
Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan pertubuhan profesional hendaklah dikekalkan. Menganggotai pertubuhan profesional atau pun forum bagi: a. meningkatkan ilmu berkaitan amalan terbaik dan sentiasa mengikuti perkembangan terkini mengenai keselamatan maklumat; b. menerima amaran awal dan nasihat berhubung kerentanan dan ancaman keselamatan maklumat terkini; c. berkongsi dan bertukar maklumat mengenai teknologi, produk, ancaman atau kerentanan; dan d. berhubung dengan kumpulan pakar keselamatan maklumat apabila berurusan dengan insiden keselamatan maklumat.	Warga Pejabat Suk Pahang (Mengikut Bidang Kepakaran)

5.7 RISIKAN ANCAMAN *(THREAT INTELLIGENCE)*	**PERANAN**
Risikan ancaman (*Threat Intelligence*) adalah serangkaian langkah dan tindakan yang diambil untuk mengesan, melindungi, dan mencegah berbagai jenis ancaman. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a. Sistem pemantauan keselamatan (*Security Monitoring*) bagi mengesan aktiviti yang mencurigakan atau ancaman perisikan yang mungkin terjadi di dalam rangkaian atau sistem. b. Memasang pendinding api *(Firewall)* bagi mengawal lalu lintas jaringan rangkaian daripada aktiviti yang mencurigakan. c. Setiap data yang disimpan hendaklah di enkripsi (*Encryption*) bagi melindungi data daripada dicapai oleh orang tidak sah. d. Memastikan setiap perisian yang digunakan adalah yang terkini dan sentiasa dikemaskini. e. Mengawal akses setiap pengguna aplikasi sistem mengikut skop tugas yang telah ditetapkan oleh pemilik sistem. f. Membahagikan rangkaian di dalam sesebuah organisasi kepada bebarapa bahagian mengikut tingkat atau sebagainya. g. Mengkaji, menilai dan mengemaskini teknologi perkakasan atau perisian mengikut dengan keadaan semasa. h. Risikan ancaman melibatkan pengumpulan, penilaian, analisis, dan pelaporan maklumat mengenai ancaman sedia ada atau baharu.	BTM
5.8 KESELAMATAN MAKLUMAT DALAM PENGURUSAN PROJEK *(INFORMATION SECURITY IN PROJECT MANAGEMENT)*	**PERANAN**
Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a. Keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek di Pejabat SUK Pahang; b. Objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek; c. Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenai pasti kawalan-kawalan yang diperlukan; dan d. Kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam polisi keselamatan siber Pejabat SUK Pahang.	Warga Pejabat SUK Pahang (Pasukan Projek)
5.9 INVENTORI MAKLUMAT DAN ASET YANG BERKAITAN	**PERANAN**

(INVENTORY OF INFORMATION AND OTHER ASSOCIATED ASSETS)	
1. Memastikan semua aset ICT Pejabat SUK Pahang hendaklah disokong dan diberi perlindungan yang bersesuaian. Perkara yang perlu dipatuhi adalah seperti berikut : a. Mengenal pasti Pegawai Penerima Aset setiap Bahagian untuk menguruskan penerimaan aset-aset ICT bagi projek-projek ICT; b. Memastikan semua aset ICT dikenal pasti, diklasifikasi, didokumen, diselenggara dan dilupuskan. Maklumat aset direkodkan dan sentiasa dikemaskini sebagaimana arahan dan peraturan yang berkuat kuasa dari semasa ke semasa; c. Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja ; d. Pegawai Aset hendaklah mengesahkan penempatan aset ICT; e. Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan; dan f. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya. 2. Aset ICT yang diselenggara hendaklah milik Pejabat SUK Pahang. Perkara yang perlu dipatuhi oleh pemilik aset adalah seperti berikut: a. Memastikan aset ICT di bawah tanggungjawabnya telah dimasukkan dalam senarai aset; b. Memastikan aset ICT telah dikelaskan dan dilindungi; c. Mengenal pasti dan mengkaji semula capaian ke atas aset penting secara berkala berdasarkan kepada polisi kawalan capaian yang telah ditetapkan; d. Memastikan pengendalian aset ICT dilaksanakan dengan baik apabila aset dihapus atau dilupuskan; dan e. Memastikan semua jenis aset dipelihara dengan baik.	Pegawai Penerima Aset, Pegawai Aset warga Pejabat SUK Pahang Pegawai Aset & warga Pejabat SUK Pahang
5.10 PENGGUNAAN MAKLUMAT DAN ASET BERKAITAN YANG BOLEH DITERIMA (*ACCEPTABLE USE OF INFORMATION AND OTHER ASSOCIATED ASSETS)*	**PERANAN**
Memastikan semua peraturan pengendalian aset dikenal pasti, didokumenkan dan dilaksanakan.	Warga Pejabat SUK Pahang
5.11 PEMULANGAN ASET (RETURN OF ASSETS)	**PERANAN**
Memastikan semua jenis aset ICT dikembalikan mengikut peraturan dan terma perkhidmatan yang ditetapkan selepas bersara, bertukar jabatan dan penamatan perkhidmatan atau kontrak.	Warga Pejabat SUK Pahang

5.12 PENGELASAN MAKLUMAT (CLASSIFICATION OF INFORMATION)	**PERANAN**
Maklumat hendaklah dikelaskan sebagaimana yang ditetapkan di dalam Prosedur Kawalan Keselamatan Dokumen. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan seperti berikut: a. Terkawal b. Terbuka	Pegawai Integriti
5.13 PELABELAN MAKLUMAT (LABELLING OF INFORMATION)	**PERANAN**
Prosedur penandaan peringkat keselamatan pada maklumat hendaklahdipatuhi berdasarkan Arahan Keselamatan.	Warga Pejabat SUK Pahang
5.14 PEMINDAHAN MAKLUMAT (INFORMATION TRANSFER)	**PERANAN**
1. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Polisi, prosedur dan kawalan pemindahan data dan maklumat yang formal hendaklah diwujudkan untuk melindungi pemindahan data dan maklumat melalui sebarang jenis kemudahan komunikasi; b. Terma pemindahan data, maklumat dan perisian antara Pejabat SUK Pahang dengan pihak luar hendaklah dimasukkan di dalam Perjanjian; c. Media yang mengandungi maklumat perlu dilindungi; dan d. Memastikan maklumat yang terdapat dalam mel elektronik hendaklah dilindungi sebaik-baiknya. 2. Pejabat SUK Pahang perlu mengambil kira keselamatan maklumat ataumenandatangani perjanjian bertulis apabila berlaku pemindahan data dan maklumat organisasi antara Pejabat SUK Pahang dengan pihak luar. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Ketua Bahagian hendaklah mengawal penghantaran dan penerimaan maklumat Pejabat SUK Pahang; b. Prosedur bagi memastikan keupayaan mengesan dan tanpa sangkalan semasa pemindahan data dan maklumat Pejabat SUK Pahang; c. Mengenai pasti pihak yang bertanggungjawab terhadap risiko pemindahan data dan maklumat sekiranya berlaku insiden keselamatan maklumat; dan d. Pejabat SUK Pahang hendaklah mengenai pasti perlindungan	Pengguna, Warga Pejabat SUK Pahang dan pembekal ICTSO, Ketua Bahagian

data dalam penggunaan, data dalam pergerakan, data dalam simpanan dan menghalang ketirisan data.	
3. Maklumat yang terlibat dalam pesanan elektronik hendaklah dilindungi sewajarnya mengikut arahan dan peraturan semasa. Perkara yang perlu dipatuhi dalam pengendalian mel elektronik dan undang-undang bertulis lain yang berkuat kuasa adalah seperti: a. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik diAgensi-agensi Kerajaan"; b. Arahan Setiausaha Majlis Keselamatan Negara Bil. 1 Tahun 2013 — Pematuhan Tatacara Penggunaan E-mel dan Internet; c. Surat Arahan Ketua Pengarah MAMPU bertarikh 1 Jun 2007 - Langkah- langkah mengenai penggunaan Mel Elektronik Agensi-agensi Kerajaan; dan d. mana-mana undang-undang bertulis Kerajaan Negeri yang berkuat kuasa;	Warga Pejabat SUK Pahang
4. Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut : a. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh Pejabat SUK Pahang sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; b. Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh Pejabat SUK Pahang; c. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; d. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul; e. Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi sepuluh megabait (10Mb) atau mengikut polisi yang ditetapkan agensi semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; f. Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui;	Warga Pejabat SUK Pahang

g. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; h. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; i. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; j. Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; k. Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera; l. Pengguna hendaklah memastikan alamat e-mel persendirian (seperti Yahoo Mail, Gmail, Hotmail dan sebagainya) tidak digunakan untuk tujuan rasmi; dan m. Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan mailbox masing-masing.	Warga Pejabat SUK Pahang
5.15 KAWALAN AKSES (ACCESS CONTROL)	**PERANAN**
1. Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu diwujudkan, didokumenkan, dan disemak berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Ia perlu dikemas kini setahun sekali atau mengikut keperluan dan menyokong peraturan kawalan capaian sedia ada. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Keperluan keselamatan aplikasi; b. Hak akses dan dasar klasifikasi maklumat sistem dan rangkaian; c. Undang-undang dan peraturan berkaitan yang berkuat kuasa semasa; d. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; e. Pengasingan peranan kawalan capaian; f. Kebenaran rasmi permintaan akses; g. Keperluan semakan hak akses berkala;	Pemilik dan Pentadbir Sistem Aplikasi

h. Pembatalan hak akses; i. Arkib semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat; dan j. Capaian *privilege.* 2. Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran dari Pejabat SUK Pahang. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a. Memastikan hanya pengguna yang dibenarkan sahaja boleh mendapat perkhidmatan rangkaian; b. Menempatkan, mengasingkan atau memasang peralatan ICT yang bersesuaian untuk kawalan keselamatan antara rangkaian Pejabat SUK Pahang, rangkaian agensi lain dan rangkaian awam; dan c. Mewujud, menguatkuasakan dan memantau mekanisme untuk pengesahan pengguna, ID pengguna, kata laluan atau peralatan ICT yang dihubungkan ke rangkaian termasuk rangkaian tanpa wayar; dan d. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	Pemilik dan Pentadbir Sistem Aplikasi
5.16 PENGURUSAN IDENTITI (IDENTITY MANAGEMENT)	**PERANAN**
Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan akses dan pembatalan hak akses. Perkara-perkara berikut hendaklah dipatuhi: a. Akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan; b. Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; c. Akaun pengguna yang diwujudkan pertama kali akan diberi capaianminimum yang akan ditetapkan oleh pemilik sistem; d. Sebarang perubahan tahap akses hendaklah mendapat kelulusan daripada pemilik perkhidmatan digital atau aplikasi terlebih dahulu; e. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; f. Penggunaan akaun milik orang lain atau akaun yang dikongsi	Semua Pengguna dan Warga Pejabat SUK Pahang

bersama adalah dilarang; dan g. Pentadbir Sistem Aplikasi/Perkhidmatan Digital boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut : i) Pengguna bercuti panjang / menghadiri kursus di luar pejabat dalam tempoh waktu melebihi tiga (3) bulan; ii) Bertukar bidang tugas kerja; iii) Bertukar ke agensi lain; iv) Bersara; atau v) Ditamatkan perkhidmatan	Semua Pengguna dan Warga Pejabat SUK Pahang
5.17 MAKLUMAT PENGESAHAN (AUTHENTICATION INFORMATION)	**PERANAN**
Peruntukan maklumat pengesahan rahsia bagi pengguna hendaklah dikawal melalui proses pengurusan formal. Peruntukan maklumat pengesahan rahsia bagi pengguna perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan.	ICTSO dan Pentadbir Perkhidmatan Aplikasi
5.18 HAK AKSES (ACCESS RIGHT)	**PERANAN**
1. Satu proses untuk penyediaan akses pengguna untuk kebenaran dan pembatalan akses pengguna ke atas semua aplikasi dan perkhidmatan ICT. 2. Pemilik aset hendaklah menyemak hak akses pengguna pada sela masa yang ditetapkan. Pentadbir Perkhidmatan Aplikasi perlu mewujudkan Prosedur/SOP berkaitan Pendaftaran dan Penamatan Pengguna sistem masing- masing sebagai rujukan semakan ke atas hak akses pengguna pada sela masa yang ditetapkan. 3. Hak akses kakitangan dan pengguna pihak luar untuk kemudahan pemprosesan data atau maklumat hendaklah dikeluarkan/dibatalkan selepas penamatan pekerjaan, kontrak atau perjanjian atau diselaraskan apabila berlaku perubahan dalam jabatan.	ICTSO dan Pentadbir Perkhidmatan Aplikasi
5.19 KESELAMATAN MAKLUMAT DALAM HUBUNGAN PEMBEKAL (INFORMATION SECURITY IN SUPPLIER RELATIONSHP)	**PERANAN**
Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset Pejabat SUK Pahang. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a. Mengenai pasti dan mendokumentasi jenis pembekal mengikut kategori; b. Proses kitaran hayat (lifecycle) yang seragam untuk menguruskan pembekal; c. Mengawal dan memantau akses pembekal;	Pengurus ICT, Pemilik Projek, Pembekal

d. Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian; e. Jenis-jenis obligasi kepada pembekal; f. Pelan kontigensi (*contingency plan*) bagi memastikan ketersediaan kemudahan pemprosesan maklumat; g. Melaksanakan program kesedaran terhadap Polisi Keselamatan Siber Pejabat SUK Pahang kepada pembekal; h. Menandatangani Surat Akuan Pematuhan Polisi Keselamatan Siber Pejabat SUK Pahang (Lampiran 3); dan i. Pembekal perlu mematuhi arahan keselamatan yang berkuatkuasa.	Pengurus ICT, Pemilik Projek, Pembekal
5.20 MENANGANI KESELAMATAN MAKLUMAT DALAM PERJANJIAN PEMBEKAL (ADDRESSING INFORMATION SECURITY WITHIN SUPPLIER AGREEMENTS)	**PERANAN**
Semua keperluan keselamatan maklumat yang berkaitan hendaklah disediakan dan dipersetujui dengan setiap pembekal yang boleh mengakses, memproses, menyimpan, menyampaikan, atau menyediakan komponen infrastruktur ICT untuk maklumat organisasi. Syarikat pembekal hendaklah memastikan semua kakitangan mereka mematuhi dan mengambil semua tindakan kawalan keselamatan yang perlu pada setiap masa dalam memberikan perkhidmatan kepada pihak Pejabat SUK Pahang selaras dengan peraturan dan kawalan keselamatan yang berkuat kuasa. Sekiranya syarikat pembekal gagal untuk mematuhi peraturan kawalan keselamatan tersebut, pihak Pejabat SUK Pahang mempunyai kuasa untuk menghalang syarikat pembekal daripada melaksanakan perkhidmatan tersebut. Perkara yang perlu dipatuhi adalah seperti yang berikut: Syarikat pembekal yang mempunyai pensijilan keselamatan yang berkaitan hendaklah diberi keutamaan; a. Pejabat SUK Pahang hendaklah memilih syarikat pembekal yang mempunyai pendaftaran sah dengan Kementerian Kewangan Malaysia dalam Kod Bidang yang berkaitan; b. Semua wakil syarikat pembekal hendaklah mempunyai kelulusan keselamatan daripada agensi berkaitan; c. Produk atau perkhidmatan yang ditawarkan oleh syarikat pembekal hendaklah melalui penilaian teknikal untuk memastikan keperluan keselamatan dipenuhi; d. Jawatankuasa Penilaian Teknikal boleh melaksanakan penilaian	Pembekal

teknikal atau bertindak ke atas penilaian pihak ketiga melalui laporan yang dikemukakan oleh syarikat pembekal; e. Laporan penilaian pihak ketiga yang dikemukakan oleh syarikat pembekal hendaklah disemak berdasarkan faktor-faktor seperti yang berikut: • Badan penilai pihak ketiga adalah bebas dan berintegriti; • Badan penilai pihak ketiga adalah kompeten; • Kriteria penilaian; • Parameter pengujian; dan • Andaian yang dibuat berkaitan dengan skop penilaian. f. Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan bagi mengakses,memproses, menyimpan, berinteraksi atau menyediakan komponen infrastruktur ICT untuk keperluan Pejabat SUK Pahang; dan g. Pembekal hendaklah mematuhi pengklasifikasian maklumat yang telah ditetapkan oleh Pejabat SUK Pahang.	Pembekal
5.21 PENGURUSAN KESELAMATAN MAKLUMAT DALAM RANTAIAN BEKALAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT) ***(MANAGING INFORMATION SECURITY IN THE INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) SUPPLY CHAIN)***	**PERANAN**
Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk mengendalikan risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk. Perkara-perkara yang perlu diambil kira adalah sepertiyang berikut: a. Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; b. Pembekal utama hendaklah memaklumkan keperluan keselamatan maklumat kepada subkontraktor atau pembekal-pembekal lain yang memberikan perkhidmatan ataupembekalan produk; dan c. Memastikan jaminan daripada pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik.	Pengurus ICT, PemilikProjek, Pembekal

5.22 **PEMANTAUAN, SEMAKAN DAN PENGURUSAN PERUBAHAN PERKHIDMATAN PEMBEKAL (MONITORING, REVIEW AND CHANGE MANAGEMENT OF SUPPLIER SERVICES)**	**PERANAN**
1. Pejabat SUK Pahang hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal secara berkala. Perkara-perkara yang perlu diambil kira adalah seperti yang berikut: a. Memantau tahap prestasi perkhidmatan untuk mengesahkanpembekal mematuhi perjanjian perkhidmatan; b. Mengkaji semula laporan perkhidmatan yang dihasilkan olehpembekal dan mengemukakan status kemajuan; dan c. Memaklumkan mengenai insiden keselamatan kepada pembekal/pemilik projek dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian. 2. Perubahan kepada peruntukan perkhidmatan oleh pembekal, termasuk mempertahan dan menambah baik dasar keselamatan maklumat sedia ada, prosedur dan kawalan, hendaklah diuruskan, dengan mengambil kira kepentingan maklumat, sistem dan proses perniagaan yang terlibat dan penilaian semula risiko. Perkara yang perlu diambil kira adalah seperti yang berikut: a. Perubahan dalam perjanjian dengan pembekal; b. Perubahan yang dilakukan oleh Pejabat SUK Pahang bagi meningkatkan perkhidmatan selaras dengan penambahbaikansistem, pengubahsuaian dasar dan prosedur; dan c. Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baru, produk-produk baru, perkakasan baru, perubahan lokasi, pertukaran pembekal dan subkontraktor.	Pengurus ICT, Pemilik Projek, Pembekal
5.23 KESELAMATAN MAKLUMAT BAGI PENGGUNAAN PERKHIDMATAN AWAN (INFORMATION SECURITY FOR USE OF CLOUD SERVICES)	**PERANAN**
Perkhidmatan awan adalah penting untuk memastikan bahawa organisasi memilih penyedia perkhidmatan awan yang mempunyai tahap keselamatan yang tinggi. Berikut adalah beberapa langkah-langkah yang diperlukan sebelum penggunaan perkhidmatan awan. 1. Menetapkan skop perolehan perkhidmatan awan yang ingin dikawal. Skop ini perlu merangkumi jenis perkhidmatan awan yang diperlukan, data yang akan dipindahkan ke awan, dan syarat-syarat keselamatan yang dikehendaki. 2. Melakukan penilaian risiko untuk mengenal pasti potensi ancaman dan	ICTSO, Pentadbir Rangkaian

kerentanan yang berkaitan dengan penggunaan perkhidmatan awan. Ini memungkinkan anda untuk mengenal pasti tahap risiko dan mengambil tindakan untuk mengurangkan risiko tersebut. 3. Memilih penyedia perkhidmatan awan yang mematuhi piawaian keselamatan maklumat dan memiliki rekod prestasi yang baik dalam bidang keselamatan dan privasi data. 4. Membuat perjanjian perkhidmatan dengan penyedia perkhidmatan awan yang mencakupi butiran keselamatanmaklumat, seperti tahap layanan, perlindungan data, pematuhan piawaian, pemisahan data, pemulihan bencana, dan pematuhan peraturan sebelum, semasa dan selepas tamat perjanjian perkhidmatan. 5. Melakukan audit keselamatan secara berkala ke atas penyedia perkhidmatan awan untuk memastikan pematuhan mereka terhadap perjanjian perkhidmatan dan piawaian keselamatan maklumat. 6. Memastikan bahawa penyedia perkhidmatan awan mempunyai perancangan pemulihan bencana yang kukuh untuk melindungi data organisasi dalam kejadian insiden yang merugikan. 7. Menilai semula keselamatan maklumat secara berkala dan memastikan ia selaras dengan keperluan keselamatan dan piawaian. 8. Memastikan bahawa organisasi mematuhi peraturan dan perundangan yang berkaitan dengan penggunaan perkhidmatan awan, terutamanya dalam hal privasi data dan perlindungan data peribadi.	ICTSO, Pentadbir Rangkaian
5.24 PERANCANGAN DAN PERSEDIAAN PENGURUSAN INSIDEN KESELAMATAN MAKLUMAT (INFORMATION SECURITY INCIDENT MANAGEMENT PLANNING AND PREPARATION)	**PERANAN**
Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan tindak balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat. Pengurusan insiden Pejabat SUK Pahang adalah berdasarkan kepada Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CSIRT Pejabat SUK Pahang yang sedang berkuat kuasa. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Memberikan kesedaran berkaitan Prosedur Operasi Standard: Pengendalian Insiden Keselamatan ICT CSIRT Pejabat SUK Pahang dan hebahan kepada warga Pejabat SUK Pahang sekiranya ada perubahan; dan b. Memastikan personel yang menguruskan insiden mempunyai tahap kompetensi yang diperlukan.	ICTSO, Pengurus ICT,CSIRT Pejabat SUK Pahang dan PemilikProjek/Sistem Aplikasi

5.25 PENILAIAN DAN KEPUTUSAN TENTANG KEJADIAN KESELAMATAN MAKLUMAT (ASSESSMENT AND DECISION ON INFORMATION SECURITY EVENTS)	**PERANAN**
Insiden keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat.	ICTSO
5.26 TINDAK BALAS TERHADAP INSIDEN KESELAMATAN MAKLUMAT (RESPONSE TO INFORMATION SECURITY INCIDENT)	**PERANAN**
Insiden keselamatan maklumat hendaklah ditangani menurut prosedur yang didokumenkan. Tindak balas terhadap insiden keselamatan maklumat adalah berdasarkan Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CSIRT Pejabat SUK Pahang. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti yang berikut: a. Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku; b. Menjalankan kajian forensik sekiranya perlu; c. Menghubungi pihak yang berkenaan dengan secepat mungkin; d. Menyimpan jejak audit, sandaran secara berkala dan melindungi integriti semua bahan bukti; e. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; f. Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; g. Menyediakan tindakan pemulihan segera; dan h. Memaklum atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu.	ICTSO, CSIRT Pejabat SUK Pahang
5.27 PEMBELAJARAN DARIPADA INSIDEN KESELAMATAN MAKLUMAT (LEARNING FROM INFORMATION SECURITY INCIDENTS)	**PERANAN**
Pengetahuan yang diperoleh daripada penganalisisan dan penyelesaian kejadian keselamatan maklumat hendaklah digunakan bagi mengurangkan kemungkinan berlakunya kejadian pada masa depan atau kesannya. Setiap insiden keselamatan maklumat perlu direkodkan dan penilaian ke atas insiden keselamatan maklumat perlu dilaksanakan untuk memastikan kawalan yang diambil adalah mencukupi atau perlu ditambah.	ICTSO, CSIRT Pejabat SUK Pahang

5.28 PENGUMPULAN BUKTI (COLLECTION OF EVIDENCE)	PERANAN
Pejabat SUK Pahang hendaklah menentukan prosedur untuk mengenai pasti koleksi, pemerolehan dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti dengan merujuk kepada arahan semasa yang berkaitan.	ICTSO, CSIRT Pejabat SUK Pahang
5.29 KESELAMATAN MAKLUMAT SEMASA GANGGUAN (INFORMATION SECURITY DURING DISRUPTION)	**PERANAN**
1. Pejabat SUK Pahang hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam situasi kecemasan, contohnya, semasa krisis atau bencana. Dalam merancang kesinambungan keselamatan maklumat, Pejabat SUK Pahang perlu mengambil kira isu-isu dalaman dan luaran yang berkaitan yang boleh memberikan kesan ke atas sistem penyampaian perkhidmatan dan fungsi Pejabat SUK Pahang. Pejabat SUK Pahang juga perlu mengambil kira keperluan dan ekspektasi pihak-pihak berkepentingan serta keperluan undang- undang dan peraturan yang terpakai. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a. Melantik pasukan tadbir urus Pengurusan Kesinambungan Perkhidmatan (PKP) Pejabat SUK Pahang; b. Menetapkan polisi PKP; c. Mengenai pasti perkhidmatan kritikal; d. Melaksanakan Kajian Impak Perkhidmatan (*Business Impact Analysis* — BIA) dan Penilaian Risiko terhadap perkhidmatan kritikal; e. Membangunkan Pelan lnduk Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak balas Kecemasan dan Pelan Pemulihan Bencana ICT. f. Melaksanakan program kesedaran dan latihan pasukan PKP dan warga Pejabat SUK Pahang; g. Melaksanakan simulasi ke atas dokumen di para (c); dan h. Melaksanakan penyelenggaraan ke atas pelan di para (c). 2. Pejabat SUK Pahang hendaklah menyediakan, mendokumenkan, melaksanakan dan menyelenggara proses, prosedur dan kawalan bagi memastikan keperluan tahap kesinambungan keselamatan maklumat ketika berada dalam keadaan yang menjejaskan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut:	Koordinator PKP, Disaster Recovery Team (DRT), Emergency Recovery Team (ERT), Critical Communication Team (CCT) Pejabat SUK Pahang Pengurusan Tertinggi Pejabat SUK Pahang, Koordinator PKP, Disaster Recovery Team (DRT),

a. Melaksanakan PKP apabila terdapat gangguan terhadap perkhidmatan kritikal Pejabat SUK Pahang yang telah dikenal pasti berdasarkan kepada Pelan Induk Pengurusan Kesinambungan Perkhidmatan, Pelan Komunikasi Krisis, Pelan Tindak balas Kecemasan dan Pelan Pemulihan Bencana ICT terkini; b. Melaksanakan post-mortem dan mengemaskini pelan-pelan PKP; c. Mengemas kini pelan-pelan PKP jika berlaku perubahan kepada fungsi kritikal Pejabat SUK Pahang; d. Mengemas kini struktur tadbir urus PKP Pejabat SUK Pahang jika berlaku pertukaran pegawai bersara dan bertukar keluar; dan e. Memastikan pasukan PKP mempunyai kompetensi yang bersesuaian dengan peranan dan tanggungjawab dalam melaksana PKP.	Emergency Recovery Team (ERT)
3. Pejabat SUK Pahang hendaklah mengesahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan pada sela masa tetap bagi memastikannya sah dan berkesan semasa situasi kecemasan.	Pengurusan Tertinggi Pejabat SUK Pahang, Koordinator PKP, Disaster Recovery Team (DRT), Emergency Recovery Team (ERT), Critical Communication Team (CCT) Pejabat SUK Pahang, Pemilik Perkhidmatan Kritikal Pejabat SUK Pahang dalam PKP dan Warga Pejabat SUK Pahang
5.30 KETERSEDIAAN ICT UNTUK KESINAMBUNGAN PERKHIDMATAN (ICT READINESS FOR BUSINESS CONTINUITY)	**PERANAN**
Teknologi Maklumat dan Komunikasi (ICT) adalah aspek penting dalam memastikan kesinambungan operasi Pejabat SUK Pahang. Ini melibatkan penyediaan infrastruktur, sistem, dan perkhidmatan ICT yang boleh diakses dan berfungsi dengan baik dalam semua keadaan, termasuk semasa krisis atau gangguan. Faktor-faktor yang perlu dipertimbangkan untuk mencapai ketersediaan ICT bagi kesinambungan Pejabat SUK Pahang adalah seperti berikut : 1. Mempunyai perancangan strategik ICT yang jelas dan menyeluruh yang mengenal pasti keperluan teknologi bagi menjayakan strategi kesinambungan perniagaan.	Pengurus ICT, ICTSO, Pentadbir Rangkaian, Pentadbir Sistem Aplikasi

2. Ini termasuk menentukan sumber daya ICT yang diperlukan, tujuan pemulihan, dan kebijakan perolehan peralatan dan perkhidmatan. 3. Mempunyai infrastruktur ICT yang *redundant*, termasuk rangkaian, pelayan, storan data, dan sokongan kuasa yang boleh berfungsi jika ada gangguan atau kegagalan. 4. Penggantian secara automatik (*failover*) dan peralatancadangan perlu dipertimbangkan. 5. Lakukan pemantauan aktif terhadap peralatan ICT untuk mengenalpasti masalah sebelum ia berlaku dan mengelakkan gangguan. 6. Pengurusan inventori peralatan, pelan pembaikan, dan pemantauan prestasi berterusan. 7. Sediakan pelan pemulihan bencana ICT yang komprehensif. Ini termasuk cadangan data, pengekalkan cadangan pelayan, dan prosedur pemulihan semula aktiviti perniagaan. 8. Ujian dan latihan berkala pelan pemulihan bencana. 9. Pastikan akses kepada sistem dan data dikawal dengan ketat dan disemak secara berkala. Ini termasuk pengurusan identiti, pengesahihan dua faktor, dan peraturan akses yang ketat. 10. Sediakan perkhidmatan pengurusan keselamatan seperti antivirus, firewall, dan pelindung kegagalan untuk menghalang ancaman keselamatan ICT. 11. Amalkan pemantauan keselamatan untuk mengenalpasti dan tindak balas kepada ancaman dan insiden keselamatan. 12. Pastikan kakitangan tahu apa yang perlu dilakukan dalam kes insiden keselamatan. 13. Melaksanakan penyelenggaraan dan pembaikan peralatan dan sistem secara berkala untuk mengelakkan kegagalan yang tidak dijangka. 14. Tetapkan jadual pembaikan berkala dan pemulihan data. 15. Pantau penggunaan sumber daya ICT seperti bandwidth dan kapasiti penyimpanan untuk mengelakkan penggunaan berlebihan yang boleh menyebabkan gangguan. 16. Pastikan penyedia perkhidmatan awan atau penyedia perkhidmatan lain mempunyai pelan kesinambungan perniagaan yang mencukupi yang dapat menyokong operasi jika berlaku gangguan.	Pengurus ICT, ICTSO, Pentadbir Rangkaian, Pentadbir Sistem Aplikasi

5.31 KEPERLUAN UNDANG-UNDANG, BERKANUN, PERATURAN DAN KONTRAK (LEGAL, STATUTORY, REGULATORY AND CONTRACTUAL REQUIREMENTS)	**PERANAN**
Keperluan perundangan, peraturan dan perjanjian kontrak hendaklah dikenal pasti dan dipatuhi oleh warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang. Keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di Pejabat SUK Pahang dan pembekal adalah seperti di Lampiran 2.	Warga Pejabat SUK Pahang, pembekal, pakar runding daripada pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang
5.32 HAK HARTA INTELEK (INTELLECTUAL PROPERTY RIGHTS)	**PERANAN**
Memastikan kepatuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelektual. Melaksanakan kawalan terhadap keperluan perlesenan supaya menggunakan perisian yang mempunyai lesen yang sah dan mematuhi had pengguna yang telah ditetapkan atau dibenarkan.	Warga Pejabat SUK Pahang, pembekal, pakar runding daripada pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang
5.33 PERLINDUNGAN REKOD (PROTECTION OF RECORDS)	**PERANAN**
Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan dan capaian ke atas orang yang tidak berkenaan seperti yang terkandung di dalam keperluan perundangan, peraturan dan perjanjian kontrak.	Warga Pejabat SUK Pahang, pembekal, pakar runding daripada pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang
5.34 KERAHSIAAN DAN PERLINDUNGAN MAKLUMAT PENGENALAN PERIBADI (PRIVACY AND PROTECTION OF PERSONAL IDENTIFIABLE INFORMATION (PII))	**PERANAN**
Pejabat SUK Pahang hendaklah memberikan jaminan dalam melindungi maklumat peribadi pengguna seperti tertakluk di dalam undang-undang dan peraturan-peraturan Kerajaan Malaysia.	Warga Pejabat SUK Pahang, pembekal, pakar runding daripada pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang
5.35 PENILAIAN KESELAMATAN MAKLUMAT OLEH PIHAK BERKECUALI (INDEPENDENT REVIEW OF INFORMATION SECURITY)	**PERANAN**
Penilaian keselamatan maklumat oleh pihak ketiga hendaklah dilaksanakan seperti yang telah dirancang atau apabila terdapat perubahan ketara terhadap sistem dan infrastruktur.	Pengurus ICT dan Pemilik Perkhidmatan Digital

5.36 PEMATUHAN POLISI, PERATURAN DAN PIAWAIAN KESELAMATAN MAKLUMAT (COMPLIANCE WITH POLICIES, RULES AND STANDARD FOR INFORMATION SECURITY)	**PERANAN**
1. Pejabat SUK Pahang hendaklah membuat kajian semula secara berkala terhadap pematuhan dasar dan standard keselamatan pemprosesan maklumat dan prosedur di kawasan yang dipertanggungjawabkan dengan polisi, piawaian dan keperluan teknikal yang bersesuaian. 2. Pejabat SUK Pahang hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti yang terkandung di dalam polisi, piawaian dan keperluan komputer.	Pengurus ICT dan Pemilik Perkhidmatan Digital
5.37 PROSEDUR OPERASI YANG DIDOKUMENKAN (DOCUMENTED OPERATING PROCEDURE)	**PERANAN**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Semua prosedur keselamatan siber yang diwujudkan, dikenal pasti dan masih diguna pakai hendaklah didokumen, disimpan dan dikawal; b. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian serta pemprosesan maklumat, pengendalian serta penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c. Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	BTM, CSIRT Pejabat SUK Pahang

6.0 KAWALAN MANUSIA (*PEOPLE CONTROL*)	
6.1 SARINGAN (*SCREENING*)	**PERANAN**
Tapisan keselamatan hendaklah dijalankan terhadap warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang yang terlibat selaras dengan keperluan perkhidmatan. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; dan b. Menjalankan tapisan keselamatan untuk Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	Warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang
6.2 TERMA DAN SYARAT PERJAWATAN (*TERMS AND CONDITION EMPLOYMENT)*	**PERANAN**
Persetujuan berkontrak dengan warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang hendaklah dinyatakan tanggungjawab mereka dan tanggungjawab organisasi terhadap keselamatan maklumat. Perkara-perkara yang mesti dipatuhi adalah seperti yang berikut: a. Menyatakan dengan lengkap dan jelas peranan serta tanggungjawab warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang yang terlibat dalam menjamin keselamatan aset ICT; dan b. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang

6.3 KESEDARAN, PENDIDIKAN DAN LATIHAN KESELAMATAN MAKLUMAT *(INFORMATION SECURITY AWARENESS AND TRAINING)*	**PERANAN**
Warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang perlu diberikan kesedaran, pendidikan dan latihan sewajarnya mengenai keselamatan aset ICT secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut : a. memastikan kesedaran, pendidikan dan latihan yang berkaitan Polisi Keselamatan Siber Pejabat SUK Pahang, Sistem Pengurusan Keselamatan Maklumat (ISMS) dan latihan teknikal yang berkaitan dengan produk/fungsi/aplikasi/sistem keselamatan secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka; b. memastikan kesedaran yang berkaitan Polisi Keselamatan Siber Pejabat SUK Pahang perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; dan c. memantapkan pengetahuan berkaitan dengan keselamatan maklumat bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan maklumat.	Warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang
6.4 PROSES TATATERTIB *(DISCIPLINARY PROCESS)*	**PERANAN**
Proses tatatertib yang formal dan disampaikan kepada warga Pejabat SUK Pahang hendaklah tersedia bagi membolehkan tindakan diambil terhadap warga Pejabat SUK Pahang yang melakukan pelanggaran keselamatan maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a. Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas warga Pejabat SUK Pahang sekiranya berlaku perlanggaran terhadap perundangan dan peraturan yang ditetapkan oleh Pejabat SUK Pahang; b. Warga Pejabat SUK Pahang yang melanggar polisi ini akan dikenakan tindakan tatatertertib atau digantung daripada mendapat capaian kepada kemudahan ICT Pejabat SUK Pahang.	Unit Integriti

6.5 TANGGUNGJAWAB SELEPAS PENAMATAN ATAU PERTUKARAN PERJAWATAN (*RESPONSIBILITIES AFTER TERMINATION OR CHANGE OF EMPLOYMENT*)	**PERANAN**
Warga Pejabat SUK Pahang yang telah tamat perkhidmatan/bertukar perkhidmatan perlu mematuhi perkara-perkara berikut: a. Memastikan semua aset ICT Pejabat SUK Pahang dikembalikan kepada Pejabat SUK Pahang mengikut peraturan dan/atau terma yang ditetapkan; b. Memastikan semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat dibatalkan oleh pentadbir sistem mengikut peraturan yang ditetapkan oleh Pejabat SUK Pahang; c. Maklumat rasmi Pejabat SUK Pahang dalam peranti tidak dibenarkan dibawa keluar dari Pejabat SUK Pahang; d. Menyedia dan menyerahkan nota serah tugas dan myPortfolio kepada penyelia yang berkaitan. Bahagian Pengurusan Sumber Manusia perlu: a. Mengemaskini semua dokumentasi berkaitan pegawai yang tamat perkhidmatan bagi memastikan kesinambungan perkhidmatan Pejabat SUK Pahang.	Warga Pejabat SUK Pahang
6.6 PERJANJIAN KERAHSIAAN (*CONFIDENTIALITY OR NON-DISCLOSURE AGREEMENTS*)	**PERANAN**
Syarat-syarat perjanjian kerahsiaan atau *non-disclosure* perlu mengambil kira keperluan organisasi dan hendaklah disemak dan dokumentasikan. Pembekal hendaklah bersetuju dan mematuhi semua keperluan keselamatan maklumat yang relevan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pembekal; b. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak pembekal perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan c. Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	ICTSO, Pentadbir Sistem Aplikasi, Pengguna dan Pembekal

6.7 TELEKERJA (*REMOTE WORKING)*	**PERANAN**
a. Capaian jarak jauh yang dimaksudkan merangkumi: i. capaian daripada sistem rangkaian dalaman; dan ii. capaian daripada sistem rangkaian luaran bagi lokasi luar pejabat untuk tujuan *teleworking*. b. Penghantaran maklumat yang menggunakan capaian jarak jauh mestilah menggunakan kaedah enkripsi (*encryption*); c. Lokasi bagi akses ke sistem aplikasi Pejabat SUK Pahang hendaklah dipastikan selamat; d. Penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada Pentadbir Rangkaian dan Keselamatan. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini; dan e. Capaian jarak jauh hendaklah menggunakan kemudahan yang disediakan oleh jabatan.	ICTSO, Pentadbir Rangkaian
6.8 PELAPORAN KEJADIAN KESELAMATAN MAKLUMAT *(INFORMATION SECURITY EVENT REPORTING)*	**PERANAN**
1. Insiden keselamatan maklumat seperti berikut hendaklah dilaporkan melalui saluran pengurusan yang betul secepat yang mungkin. Insiden keselamatan siber atau ancaman yang berlaku hendaklah dilaporkan kepada CSIRT Pejabat SUK Pahang kemudiannya perlu melaporkan kepada ICTSO dengan kadar segera. Perkara yang perlu dipertimbangkan adalahseperti yang berikut: a. Maklumat didapati atau disyaki hilang, atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c. Kata laluan atau mekanisme kawalan akses didapati atau disyaki hilang, dicuri atau didedahkan; d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan e. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka. Prosedur pelaporan insiden keselamatan Siber berdasarkan: a. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan	Warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang

Insiden Keselamatan Teknologi Maklumat dan Komunikasi; b. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam; c. Surat Arahan CIO 18 Februari 2011 – Proses Kerja Pelaporan Insiden Keselamatan ICT *Computer Emergency Response Team* (CSIRT) Pejabat SUK Pahang; d. Prosedur Operasi Standard: Pengurusan Pengendalian Insiden Keselamatan ICT CSIRT Pejabat SUK Pahang; dan e. Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan Dan Pengendalian Insiden Keselamatan Siber Sektor Awam. f. Akta Keselamatan Siber 2024 dan Peraturan-peraturan [Akta 854]	
2. Insiden keselamatan maklumat hendaklah dinilai dan ditentukan jika perlu dikelaskan sebagai insiden keselamatan maklumat.	ICTSO

7.0 KAWALAN FIZIKAL (*PHYSICAL CONTROL*)	
7.1 PERIMETER KESELAMATAN FIZIKAL (*PHYSICAL SECURITY PERIMETERS)*	**PERANAN**
Ini bertujuan untuk menghalang akses tanpa kebenaran serta kerosakan dan gangguan secara fizikal terhadap premis, maklumat dan Aset ICT Pejabat SUK Pahang. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Menggunakan keselamatan perimeter (halangan seperti dinding, pagar, kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; b. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; c. Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; d. Mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacaubilau manusia dan sebarang bencana alam atau perbuatan manusia; e. Melaksanakan perlindungan fizikal dan menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; f. Memastikan kawasan-kawasan penghantaran danpemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya; dan g. Memasang alat penggera atau kamera keselamatan;	BKP
7.2 KEMASUKAN FIZIKAL (*PHYSICAL ENTRY*)	**PERANAN**
1. Kawalan kemasukan fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis Pejabat SUK Pahang. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a. Setiap warga Pejabat SUK Pahang hendaklah mempamerkan pas keselamatan sepanjang waktu bertugas; b. Semua pas keselamatan hendaklah diserahkan kembali kepada jabatan apabila pengguna bertukar, tamat perkhidmatan atau bersara; c. Setiap pelawat boleh mendapatkan Pas Keselamatan Pelawat di Lobi Kaunter Perkhidmatan Pejabat SUK Pahang terlebih dahulu	Warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang

dan hendaklah dikembalikan semula selepas tamat lawatan; d. Kehilangan pas mestilah dilaporkan dengan segera; dan e. Hanya pengguna yang diberi kebenaran sahaja boleh menggunakan Aset ICT Pejabat SUK Pahang. 2. Titik kemasukan (*access point)* seperti kawasan penyerahan dan pemunggahan serta kawasan larangan hendaklah dikawal dan jika boleh diasingkan daripada kemudahan pemprosesan maklumat bagi mengelakkan kemasukan yang tidak dibenarkan. 3. Pejabat SUK Pahang hendaklah memastikan kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada dimasuki oleh pihak yang tidak diberi kebenaran.	BKP
7.3 KESELAMATAN PEJABAT, BILIK DAN KEMUDAHAN (*SECURING OFFICES, ROOMS AND FACILITIES)*	**PERANAN**
Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah dirangka dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Kawasan tempat bekerja, bilik mesyuarat, bilik krisis, bilik perbincangan, bilik fail, bilik cetakan, bilik kawalan CCTV dan pusat data perlu dihadkan daripada diakses tanpa kebenaran; b. Kawasan tempat berkerja, bilik dan tempat operasi ICT perlu dihadkan daripada diakses oleh orang luar; dan c. Petunjuk lokasi bilik operasi dan tempat larangan haruslah mematuhi arahan keselamatan.	Warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang
7.4 PEMANTAUAN KESELAMATAN FIZIKAL (*PHYSICAL SECURITY MONITORING)*	**PERANAN**
Akses tanpa kebenaran ke kawasan fizikal terhad seperti bilik pelayan dan bilik peralatan IT boleh mengakibatkan kehilangan kerahsiaan, ketersediaan, integriti dan keselamatan aset maklumat. Berikut adalah kawalan yang boleh dilaksanakan: a. Kamera CCTV b. Pengawal keselamatan c. Penggera keselamatan untuk penceroboh d. Alat perisian untuk pengurusan keselamatan fizikal	Pentadbir Pusat Data dan BKP
7.5 PERLINDUNGAN DARI ANCAMAN FIZIKAL DAN PERSEKITARAN (*PROTECTION AGAINST PHYSICAL AND ENVIRONMENTAL THREATS*)	**PERANAN**
Perlindungan fizikal terhadap bencana alam, serangan berniat jahat atau kemalangan hendaklah dirangka dan dilaksanakan. Pejabat SUK Pahang	Pentadbir Pusat Data dan BKP

perlu mereka bentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau bilau dan bencana.	
7.6 BEKERJA DI KAWASAN YANG SELAMAT (*WORKING INSECURE AREA*)	**PERANAN**
Prosedur bekerja di kawasan selamat hendaklah dirangka dan dilaksanakan. Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan bagi warga Pejabat SUK Pahang yang tertentu sahaja. Ini dilakukan untuk melindungi aset ICT yang terdapat dalam premis Pejabat SUK Pahang termasuklah Pusat Data. Kawasan ini mestilah dilindungi daripada sebarang ancaman, kelemahan dan risiko seperti pencerobohan, kebakaran dan bencanaalam. Kawalan keselamatan ke atas kawasan tersebut adalah seperti yang berikut: a. Sumber data atau server, peralatan komunikasi dan storan perlu ditempatkan di pusat data, bilik server atau bilik khas yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegahan kebakaran; b. Akses adalah terhad kepada warga Pejabat SUK Pahang yang telahdiberi kuasa sahaja dan dipantau pada setiap masa; c. Pemantauan dibuat menggunakan *Closed-Circuit Television* (CCTV) kamera atau lain-lain peralatan yang sesuai; d. Peralatan keselamatan (CCTV, log akses) perlu diperiksa secara berjadual; e. Butiran pelawat yang keluar masuk ke kawasan larangan perlu direkodkan; f. Pelawat yang dibawa masuk mesti diawasi oleh pegawai yang bertanggungjawab di sepanjang tempoh di lokasi berkaitan; g. Lokasi premis ICT hendaklah tidak berhampiran dengan kawasan pemunggahan, saliran air dan laluan awam; h. Memperkukuh tingkap dan pintu serta dikunci untuk mengawal kemasukan; i. Memperkukuh dinding dan siling; dan j. Mengehadkan jalan keluar masuk.	Pentadbir Pusat Data dan BKP
7.7 MEJA KOSONG DAN SKRIN KOSONG (*CLEAR DESK AND CLEAR SCREEN)*	**PERANAN**
Dasar meja kosong untuk kertas dan media penyimpanan boleh alih serta dasar skrin kosong untuk kemudahan pemprosesan maklumat hendaklah digunakan. Semua maklumat dalam apa jua bentuk media hendaklah	Warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang

disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Menggunakan kemudahan *screen saver password* atau *logout* apabila meninggalkan komputer; b. Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan c. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat. d. E-mel masuk dan keluar hendaklah dikawal; dan e. Menghalang penggunaan tanpa kebenaran bagi peralatan seperti mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital.	mempunyai urusan dengan perkhidmatanICT Pejabat SUK Pahang
7.8 PENEMPATAN DAN PERLINDUNGAN PERALATAN (*EQUIPMENT SITING AND PROTECTION)*	**PERANAN**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b. Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; c. Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasanICT yang telah ditetapkan; d. Pengguna dilarangmembuat instalasi sebarang perisian tambahan tanpa kebenaran Pegawai Aset ICT / Ketua Jabatan; e. Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; f. Pengguna mesti memastikan perisian *antivirus* di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan;	Warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang

g. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; h. Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; i. Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS) dan *Generator Set (Gen-Set*); j. Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-cirikeselamatan. Peralatan rangkaian seperti *switches, router* dan lain-lain perlu diletakkan di dalam rak khas; k. Semua peralatan yang digunakan secara berterusan tanpa henti mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; l. Peralatan ICT yang hendak dibawa keluar dari premis jabatan perlu mendapat kelulusan Pegawai Aset ICT dan direkodkan bagi tujuan pemantauan; m. Peralatan ICT yang hilang hendaklah dilaporkan kepada Pegawai Aset ICT dengan segera; n. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; o. Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pegawai Aset ICT; p. Sebarang kerosakan peralatan ICT hendaklah dilaporkanmelalui Sistem Meja Bantuan ICT: **(**https://aduanict.pahang.gov.my/**)** untuk dibaik pulih; q. Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan pada semua Aset ICT. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; r. Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; s. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; t. Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalamkeadaan "OFF" apabila meninggalkan pejabat;	Warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang

u. Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ketua jabatan; dan v. Memastikan plag dicabut daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya. w. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya yang digunakan sepenuhnya bagi urusan rasmi sahaja.	Warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang
7.9 KESELAMATAN ASET DI LUAR PREMIS (*SECURITY OF ASSETS OF PREMISES)*	**PERANAN**
Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis Pejabat SUK Pahang. Peralatan yang dibawa keluar dari premis Pejabat SUK Pahang adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalahseperti yang berikut: a. Peminjam perlu bertanggungjawab terhadap keselamatan Aset ICT yang dipinjam; b. Aset ICT perlu dilindungi dan dikawal sepanjang masa; c. Penyimpanan atau penempatan Aset ICT perlu mengambil kira ciri-ciri keselamatan lokasi yang bersesuaian; dan d. Sebarang kehilangan semasa peminjaman Aset ICT tersebut perlulah dilaporkan kepada pihak Berkuasa dan kepada Pegawai Aset ICT.	Warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang
7.10 MEDIA STORAN (*STORAGE MEDIA*)	**PERANAN**
1. Prosedur pengurusan media boleh alih hendaklah dilaksanakan mengikut skim pengkelasan yang diguna pakai oleh Pejabat SUK Pahang. Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti yang berikut: a. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b. Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; d. Mengawal dan merekod aktiviti penyelenggaraan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan	Pentadbir Sistem Aplikasi dan Pengguna

e. Menyimpan semua jenis media di tempat yang selamat.	
2. Prosedur pelupusan media adalah seperti berikut: a. Pelupusan media perlu mendapat kelulusan dan mengikut kaedah pelupusan aset ICT yang ditetapkan oleh Pejabat SUK Pahang. b. Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dihapuskan atau dimusnahkan mengikut prosedur yang berkuat kuasa.	Pentadbir Sistem Aplikasi dan Jawatankuasa yang dilantik untuk pelupusan aset.
3. Prosedur pemindahan media fizikal adalah sperti berikut: a. Pemindahan media fizikal keluar premis perlu mendapat kelulusan dan mengikut kaedah pemindahan aset ICT yang ditetapkan oleh Pejabat SUK Pahang. b. Media yang mengandungi maklumat terperingkat hendaklah disanitasikan terlebih dahulu sebelum dipindahkan mengikut prosedur yang berkuat kuasa	Pemilik media
4. Kelengkapan, maklumat atau perisian tidak boleh dibawa keluar dari tempatnya tanpa mendapat kebenaran terlebih dahulu. Aset ICT yang dibawa untuk kegunaan di luar pejabatadalah terdedah kepada pelbagai risiko. Langkah-langkah berikut boleh diambil untuk menjamin keselamatan Aset ICT: a. Aset ICT yang dibawa keluar dari premis Pejabat SUK Pahang mestilah mendapat kelulusan Pegawai Aset ICT atau Ketua Bahagian/Unit atau Pengurus ICT dan tertakluk kepada tujuan yang dibenarkan; b. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan;	Pengguna, Pegawai Aset
7.11 UTILITI SOKONGAN (*SUPPORTING UTILITIES*)	**PERANAN**
Peralatan ICT hendaklah dilindungi daripada kegagalan kuasa dan gangguan Iain yang disebabkan oleh kegagalan utiliti sokongan. Semuaalat sokongan perlu diselenggara dari semasa ke semasa (sekurang-kurangnya setahun sekali).	Warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang

7.12 KESELAMATAN KABEL (*CABLING SECURITY*)	PERANAN
Kabel kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada pintasan, gangguan atau kerosakan. Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Langkah- langkah keselamatan yang perlu diambil adalah seperti yang berikut: a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*, dan d. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan bencana dan pintasan maklumat.	BTM, BKP
7.13 PENYELENGGARAAN PERKAKASAN (*EQUIPMENT MAINTENANCE)*	**PERANAN**
Peralatan ICT hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti yang berterusan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi yang telah ditetapkan oleh pengeluar; b. Memastikan perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; c. Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; e. Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; f. Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan g. Semua penyelenggaraan mestilah mendapat kebenaran daripada Pegawai Aset ICT.	Pentadbir Teknikal

7.14 PELUPUSAN SELAMAT ATAU PENGGUNAAN SEMULA PERALATAN (*SECURE DISPOSAL OR RE-USE OF EQUIPMENT*)	PERANAN
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh Pejabat SUK Pahang dan ditempatkan di bahagian/unit atau Jabatan Kerajaan Negeri. Semua peralatan yang mengandungi media penyimpanan hendaklah dipastikan bahawa data yang sensitif dan perisian berlesen telah dikeluarkan atau berjaya ditulis ganti (overwrite) sebelum dilupuskan atau diguna semula. Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh Pejabat SUK Pahang dan ditempatkan di Pejabat SUK Pahang. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan di agensi dan jabatan masing-masingPejabat SUK Pahang.. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu dengan cara yang selamat; b. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; c. Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; d. Pegawai Aset ICT hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; e. Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; f. Pegawai Aset ICT bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam Sistem Pengurusan Aset; g. Pelupusan peralatan ICT Pejabat SUK Pahang hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan h. Pengguna ICT adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti berikut:	Pegawai Aset ICT dan Warga Pejabat SUK Pahang

1. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, hardisk, motherboard dan sebagainya; 2. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke lokasi berlainan tanpa kebenaran; 3. Memindah keluar dari Agensi atau Jabatan bagi mana-mana peralatan ICT milik Pejabat SUK Pahang yang hendak dilupuskan tanpa kebenaran; 4. Melupuskan sendiri peralatan ICT Pejabat SUK Pahang kerana kerja-kerja pelupusan di bawah tanggungjawab Pejabat SUK Pahang; dan 5. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti thumb drive atau external hard disk sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	Pegawai Aset ICT dan Warga Pejabat SUK Pahang

8 KAWALAN TEKNOLOGI (*TECHNOLOGICAL CONTROL*)	
8.1 PERANTI PENGGUNA (*USER END POINT DEVICES*)	**PERANAN**
1. Pengguna hendaklah memastikan kelengkapan yang dibiarkan tanpa kawalan mempunyai perlindungan sewajarnya. Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut: a. Tamatkan sesi aktif apabila selesai tugas; b. *Log-off* komputer meja, komputer riba dan pelayan apabila sesi bertugas selesai; dan c. Komputer meja, komputer riba atau terminal selamat daripada pengguna yang tidak dibenarkan. 2. Keselamatan maklumat hendaklah diberi perhatian dalam semua jenis pengurusan projek. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut: a. Keselamatan maklumat perlu diintegrasikan bagi setiap pengurusan projek di Pejabat SUK Pahang; b. Objektif keselamatan maklumat hendaklah diambil kira dalam pengurusan projek merangkumi semua fasa pelaksanaan metodologi projek; c. Pengurusan risiko ke atas keselamatan maklumat hendaklah dikendalikan di awal projek untuk mengenai pasti kawalan-kawalanyang diperlukan; dan d. Kontrak hendaklah mengandungi semua bidang yang terpakai dalam keperluan keselamatan maklumat seperti yang terkandung dalam polisi keselamatan siber Pejabat SUK Pahang.	Warga Pejabat SUK Pahang, pembekal,pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang
8.2 HAK AKSES ISTIMEWA (*PRIVILEGED ACCESS RIGHT*)	**PERANAN**
Hak akses istimewa membolehkan Pejabat SUK Pahang mengawal akses kepada infrastruktur, aplikasi, aset Pejabat SUK Pahang dan mengekalkan integriti semua data dan sistem yang disimpan. Pejabat SUK Pahang hendaklah: a. Kenal pasti senarai pengguna yang memerlukan sebarang tahap akses istimewa – sama ada untuk sistem individu – seperti pangkalan data – aplikasi atau OS asas. b. Kekalkan dasar yang memperuntukkan hak akses istimewa	Pengguna, Pentadbir Perkhidmatan Aplikasi, ICTSO

kepada pengguna pada apa yang dikenali sebagai "acara mengikut acara asas" - pengguna harus diberikan tahap akses berdasarkan minimum yang diperlukan untuk mereka menjalankan peranan mereka. c. Menggariskan proses kebenaran yang jelas yang berurusan dengan semua permintaan untuk akses istimewa, termasuk menyimpan rekod semua hak akses yang telah dilaksanakan. d. Pastikan hak akses tertakluk pada tarikh luput yang berkaitan. e. Ambil langkah untuk memastikan bahawa pengguna mengetahui dengan jelas sebarang tempoh masa di mana mereka beroperasi dengan akses istimewa kepada sistem. f. Jika berkaitan, pengguna diminta untuk mengesahkan semula sebelummenggunakan hak akses istimewa, untuk menjejaskan keselamatan maklumat/data yang lebih besar. g. Menjalankan audit berkala ke atas hak akses istimewa, terutamanya selepas tempoh perubahan jabatan. Hak akses pengguna harus disemak berdasarkan "tugas, peranan, tanggungjawab dan kecekapan" mereka. h. Pertimbangkan untuk beroperasi dengan memastikan hak akses istimewa diberikan dalam tetingkap masa yang dikawal ketat yang memenuhi keperluan minimum untuk operasi yang akan dijalankan (perubahan kritikal, pentadbiran sistem dsb). i. Pastikan semua aktiviti akses istimewa dicatatkan dengan sewajarnya. j. Cegah penggunaan maklumat log masuk sistem generik (terutamanyanama pengguna dan kata laluan piawai). k. Mematuhi dasar memberikan pengguna dengan identiti yang berasingan, yang membolehkan kawalan yang lebih ketat ke atas hakakses istimewa. Identiti sedemikian kemudiannya boleh dikumpulkan bersama, dengan kumpulan yang berkaitan diberikan tahap hak aksesyang berbeza. l. Pastikan hak akses istimewa dikhaskan untuk tugas kritikal sahaja, yang berkaitan dengan operasi berterusan rangkaian ICT yang berfungsi – seperti pentadbiran sistem dan penyelenggaraan rangkaian.	Pengguna, Pentadbir Perkhidmatan Aplikasi, ICTSO

8.3 SEKATAN AKSES MAKLUMAT (*INFORMATION ACCESS RESTRICTION)*	**PERANAN**
Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut dasar kawalan capaian.	Pengguna, Pentadbir Perkhidmatan Aplikasi, ICTSO
8.4 AKSES KEPADA KOD SUMBER (*ACCESS TO SOURCE CODE*)	**PERANAN**
Capaian kepada kod sumber hendaklah dihadkan. Perkara-perkara yang perlu dipertimbangkan adalah seperti yang berikut: a. Log audit perlu dikekalkan kepada semua akses kepada kod sumber; b. Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada kawalan perubahan; dan c. Kod sumber (*source code*) bagi semua aplikasi dan perisian adalah menjadi hak milik Pejabat SUK Pahang.	Pengarah Projek, Pengurus Projek dan Pentadbir Perkhidmatan Digital
8.5 PENGESAHAN KESELAMATAN (*SECURE AUTHENTICATION*)	**PERANAN**
Kawalan capaian terhadap sistem aplikasi perlu mempunyai kaedah pengesahan log masuk yang selamat dan bersesuaian bagi mengelakkan sebarang capaian yang tidak dibenarkan. Langkah dan kaedah kawalan yang digunakan adalah seperti yang berikut: a. Mengesahkan pengguna yang dibenarkan selaras dengan peraturan jabatan; b. Menjana amaran (*alert*) sekiranya berlaku perlanggaran semasa proses log masuk terhadap aplikasi sistem; c. Mengawal capaian ke atas aplikasi sistem menggunakan prosedur log masuk yang terjamin; d. Mewujudkan satu teknik pengesahan yang bersesuaian bagi mengesahkan pengenalan diri pengguna; e. Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : i. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; ii. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; iii. Panjang kata laluan mestilah sekurang-kurangnya DUA	Pentadbir Perkhidmatan Digital, ICTSO

BELAS (12) AKSARA dengan gabungan antara huruf, aksara khas dan nombor (alphanumeric) KECUALI bagi perkakasan dan perisian yang mempunyai pengurusan kata laluan yang terhad; iv. Kata laluan tidak boleh didedahkan dengan apa cara sekalipun; v. Kata laluan papan kekunci (lock screen) dan screen saver hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; vi. Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam atur cara; vii. Bagi sistem aplikasi, kuatkuasakan pertukaran kata laluan semasa login kali pertama atau selepas login kali pertama atau selepas kata laluan diset semula; viii. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; ix. Bagi sistem aplikasi, had cubaan kemasukan kata laluan bagi capaian adalah maksimum tiga (3) kali sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan dibekukan. Kemasukan kata laluan seterusnya hanya boleh dibuat selepas bagi tempoh masa tertentu (mengikut kesesuaian sistem) atau setelah diset semula oleh Pentadbir Sistem Aplikasi/Perkhidmatan Digital; x. Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; xi. Sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna. f. Mewujudkan jejak audit ke atas semua capaian aplikasi sistem.	Pentadbir Perkhidmatan Digital, ICTSO
8.6 PENGURUSAN KAPASITI (*CAPACITY MANAGEMENT*)	**PERANAN**
Penggunaan sumber hendaklah dipantau, disesuaikan dan unjuran hendaklah disediakan untuk keperluan keupayaan masa hadapan bagi memastikan prestasi sistem yang dikehendaki dicapai. Perkara-perkara yang perlu dipatuhi adalah seperti berikut :	Pemilik Sistem Aplikasi, Pentadbir Sistem Aplikasi

a. Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan b. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan siber bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pemilik Sistem Aplikasi, Pentadbir Sistem Aplikasi
8.7 PERLINDUNGAN DARIPADA PERISIAN HASAD (*PROTECTION AGAINST MALWARE)*	**PERANAN**
Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan dari serangan malware hendaklah dilaksanakan dan digabungkan dengan kesedaran pengguna terhadap serangan tersebut. Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan aset ICT daripada perisian berbahaya adalah seperti berikut : a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti Antivirus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS), *Content filtering* dan *Web Application Firewall (WAF)* serta mengikut prosedur penggunaan yang betul dan selamat; b. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; c. Memastikan perisian antivirus mempunyai pengurusan berpusat bagi memudahkan penetapan polisi dan penyediaan laporan jika berlaku *virus outbreak* dalam rangkaian; d. Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya serta dilaksanakan secara berkala; dan e. Mengemas kini antivirus dengan signature/*pattern* terkini.	Pentadbir Teknikal, Pentadbir Rangkaian, Pengguna
8.8 PENGURUSAN KERENTANAN TEKNIKAL (*MANAGEMENT OF TECHNICAL VULNERABILITIES)*	**PERANAN**
1. Maklumat tentang kerentanan teknikal sistem maklumat yang digunakan hendaklah diperoleh pada masa yang tepat, pendedahan jabatan terhadap kerentanan tersebut hendaklah dinilai dan langkah-langkah yang sesuai hendaklah diambil untuk menangani risiko yang berkaitan.	Pentadbir Sistem Aplikasi dan CSIRT Pejabat SUK Pahang

Kawalan terhadap keterdedahan teknikal perlu dilaksanakan ke atas sistem aplikasi dan operasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Melaksanakan ujian penembusan untuk memperoleh maklumat kerentanan teknikal bagi sistem aplikasi dan operasi; b. Menganalisis tahap risiko kerentanan; dan c. Mengambil tindakan pengolahan dan kawalan risiko. 2. Pejabat SUK Pahang hendaklah membuat kajian semula secara berkala terhadap pematuhan pemprosesan maklumat dan prosedur seperti yang terkandung dalam polisi, piawaian dan keperluan komputer.	Pengurus ICT dan Pemilik Perkhidmatan Digital
8.9 PENGURUSAN KONFIGURASI (*CONFIGURATION MANAGEMENT)*	**PERANAN**
Pengurusan konfigurasi ialah bahagian penting dalam operasi pengurusan aset organisasi yang lebih luas. Konfigurasi adalah kunci dalam memastikan rangkaian bukan sahaja beroperasi sebagaimana mestinya, tetapi juga dalam melindungi peranti daripada perubahan yang tidak dibenarkan atau pindaan yang salah di pihak kakitangan penyelenggaraan dan/atau vendor. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Cuba untuk menggunakan panduan khusus vendor dan/atau sumber terbuka yang tersedia secara umum tentang cara terbaikuntuk mengkonfigurasi aset perkakasan dan perisian. b. Memenuhi keperluan keselamatan minimum untuk peranti, aplikasi atau sistem yang sesuai untuknya. c. Bekerja selaras dengan usaha keselamatan maklumat organisasi yang lebih luas, termasuk semua kawalan ISO yang berkaitan. d. Perlu diingat keperluan perniagaan unik jabatan - terutamanya dalam hal konfigurasi keselamatan - termasuk kebolehlaksanaan untuk menggunakan atau mengurus templat pada bila-bila masa. e. Disemak pada selang masa yang sesuai untuk memenuhi kemas kini sistem dan/atau perkakasan, atau sebarang ancaman keselamatan yang berlaku.	ICTSO dan Pentadbir Sistem Aplikasi
8.10 PENGHAPUSAN MAKLUMAT (*INFORMATION DELETION*)	**PERANAN**
Organisasi harus sedar tentang kewajipan mereka untuk memadamkan data yang disimpan pada *server*, *hard disk*, *data array* dan *USB* apabila ia tidak lagi diperlukan dengan:	ICTSO dan Pentadbir Sistem Aplikasi

a. Pilih kaedah pemadaman yang sesuai yang mematuhi mana-mana undang-undang atau peraturan sedia ada. Pilihan termasuk pemadaman biasa, tulis ganti atau penghapusan dikodkan. Pastikan bahawa, apabila menggunakan vendor pemadaman khusus, organisasi memperoleh bukti yang mencukupi (biasanya melalui dokumentasi) bahawa pemadaman telah dilakukan. b. Organisasi harus menyatakan dengan tepat keperluan mereka apabila menggunakan vendor pihak ketiga, termasuk kaedah pemadaman dan jangka masa, dan harus menjamin bahawa aktiviti pemadaman dimasukkan dalam kontrak yang mengikat.	ICTSO dan Pentadbir Sistem Aplikasi
8.11 PELITUPAN DATA (*DATA MASKING*)	**PERANAN**
Apabila menggunakan salah satu daripada teknik ini, organisasi harus mempertimbangkan: a. Tahap pelitupan dan/atau penyamaran yang diperlukan, berbanding dengan sifat data. b. Cara *data masking* sedang diakses. c. Sebarang perjanjian mengikat yang menyekat penggunaan datauntuk disembunyikan. d. Mengekalkan *data masking* berasingan daripada mana-mana jenis data lain, untuk mengelakkan subjek data dikenal pasti dengan mudah. e. Meneliti data yang diterima, dan bagaimana ia telah diberikan kepada mana-mana sumber dalaman atau luaran.	ICTSO dan Pentadbir Sistem Aplikasi
8.12 PENCEGAHAN KEBOCORAN DATA (*DATA LEAKAGE PREVENTION)*	**PERANAN**
Kebocoran data sukar untuk dihapuskan sepenuhnya. Walau bagaimanapun, untuk meminimumkan risiko yang unik untuk operasi perkhidmatan, jabatan harus: a. Klasifikasikan data selaras dengan piawaian industri yang diiktiraf (PII, data komersial, maklumat produk), untuk menetapkan tahap risiko yang berbeza-beza di seluruh bahagian. b. Memantau dengan teliti saluran data yang diketahui yang banyak digunakan dan terdedah kepada kebocoran (cth. e-mel, pemindahan fail dalaman dan luaran, peranti USB).	ICTSO, Pentadbir Sistem Aplikasi, Pentadbir Rangkaian

c. Hadkan keupayaan pengguna untuk menyalin dan menampal data (jika berkenaan) ke dan dari platform dan sistem tertentu. d. Kebenaran daripada pemilik data sebelum sebarang pemindahan data dilaksanakan. e. Pertimbangkan untuk mengurus atau menghalang pengguna daripada mengambil tangkapan skrin atau mengambil gambar monitor yang memaparkan jenis data yang dilindungi. f. Sulitkan sandaran yang mengandungi maklumat sensitif. g. Merangka langkah keselamatan pintu masuk dan langkah pencegahan kebocoran yang melindungi daripada faktor luaran seperti (tetapi tidak terhad kepada) pengintipan industri, sabotaj, gangguan komersial dan/atau kecurian IP. h. Memastikan perisian operating sistem dan antivirus sentiasa dikemaskini.	ICTSO, Pentadbir Sistem Aplikasi, Pentadbir Rangkaian
8.13 SANDARAN MAKLUMAT *(INFORMATION BACKUP*)	**PERANAN**
Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara tetap menurut prosedur sandaran yang dipersetujui. Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Membuat *backup* keselamatan ke atas semua sistem perisian danaplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b. Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat; c. Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu bencana. d. Sandaran hendaklah dilaksanakan mengikut jadual yang dirancangsama ada secara harian, mingguan, bulanan atau tahunan. Kekerapan sandaran bergantung pada tahap kritikal maklumat, dan hendaklah disimpan sekurang-kurangnya tiga (3) generasi *backup*; dan e. Merekod dan menyimpan salinan *backup* di lokasi yang berlainan (*off-site*) dan selamat.	Pentadbir Sistem Aplikasi, Pentadbir Pusat Data

8.14 KETERSEDIAAN KEMUDAHAN PEMPROSESAN MAKLUMAT (*REDUNDANCY OF INFORMATION PROCESSING FACILITIES*)	**PERANAN**
Kemudahan pemprosesan maklumat Pejabat SUK Pahang perlu mempunyai lewahan yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan lewahan perlu diuji (*failover test*) keberkesanannya dari semasa ke semasa.	Pentadbir Pusat Data,Pemilik Perkhidmatan Digital dan Pentadbir Sistem Aplikasi
8.15 LOGGING (*LOGGING*)	**PERANAN**
1. Log peristiwa yang merekodkan aktiviti pengguna, pengecualian, ralat dan peristiwa keselamatan maklumat hendaklah disediakan, disimpan dan dikaji semula secara tetap. Log sistem ICT ialah bukti yang didokumenkan dan merupakan turutan kejadian bagi setiap aktiviti yang berlaku pada sistem. Log ini hendaklah mengandungi maklumat seperti pengenalpastian terhadap capaian yang tidak dibenarkan, aktiviti- aktiviti yang tidaknormal serta aktiviti-aktiviti yang tidak dapat dijelaskan. Log hendaklah disimpan dan direkodkan selaras dengan arahan/pekeliling terkini yang dikeluarkan oleh Kerajaan. Log hendaklah dikawal bagi mengekalkan integriti data. Jenis fail log bagi server dan aplikasi yang perlu diaktifkan adalah seperti berikut : a. fail log sistem pengoperasian; b. fail log servis (web, e-mel); c. fail log aplikasi (*audit trail*); dan d. fail log rangkaian (*switch, firewall*, IPS)	Pentadbir SistemAplikasi
Pentadbir Sistem Aplikasi/Perkhidmatan Digital hendaklah melaksanakan perkara-perkara berikut : a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; b. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakanmembaik pulih dengan segera; dan c. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem hendaklah melaporkan kepada CSIRT Pejabat SUK Pahang.	Pentadbir Sistem Aplikasi
2. Kemudahan pengelogan dan maklumat log hendaklah dilindungi daripada ubahan dan capaian tanpa izin. 3. Aktiviti pentadbir sistem dan pengendali sistem hendaklah direkodkan dan log aktiviti tersebut hendaklah dilindungi dan dikaji semula	Pentadbir Sistem Aplikasi dan CSIRT Pejabat SUK Pahang

secara tetap. a. Memantau penggunaan kemudahan memproses maklumat secara berkala; b. Aktiviti pentadbir dan pengendali sistem perlu direkodkan. Aktiviti log hendaklah dilindungi dan catatan jejak audit disemak dari semasa ke semasa dan menyediakan laporan jika perlu; c. Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; d. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; e. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem hendaklah melaporkan kepada Pasukan CSIRT Pejabat SUK Pahang.	Pentadbir Sistem Aplikasi dan CSIRT Pejabat SUK Pahang
8.16 AKTIVITI PEMANTAUAN (*MONITORING ACTIVITIES*)	**PERANAN**
Pejabat SUK Pahang hendaklah memasukkan perkara berikut dalam operasipemantauan jabatan: a. Kedua-dua trafik rangkaian masuk dan keluar, termasuk data ke dan dari aplikasi; b. Akses kepada platform kritikal organisasi, termasuk (tetapi tidakterhad kepada Sistem, Pelayan, Perkakasan rangkaian); c. Sistem pemantauan itu sendiri; d. Fail konfigurasi; e. Log peristiwa daripada peralatan keselamatan dan platform perisian; f. Semakan kod yang memastikan mana-mana program boleh digunakan adalah dibenarkan dan bebas daripada ancaman; g. Pengiraan, penyimpanan dan penggunaan sumber rangkaian.	ICTSO, Pentadbir Rangkaian
8.17 PENYEGERAKKAN JAM (*CLOCK SYNCHRONISATION*)	**PERANAN**
Jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain jabatan atau domain keselamatan hendaklah disegerakkan mengikut sumber rujukan masa tunggal.	Pentadbir Pusat Data, Pentadbir Rangkaian, Pentadbir Teknikal

Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam Pejabat SUK Pahang atau domain keselamatan perlu diseragamkan dengan satu sumber waktu yang ditetapkan oleh *National Metrology Institute of Malaysia* (NMIM).	Pentadbir Pusat Data, Pentadbir Rangkaian, Pentadbir Teknikal
8.18 PENGGUNAAN UITILITI PROGRAM ISTIMEWA (*USE OF PRIVILEGED UTILITY PROGRAMS)*	**PERANAN**
Untuk mengekalkan integriti rangkaian dan meningkatkan kesinambungan perniagaan, Pejabat SUK Pahang hendaklah: a. Hadkan penggunaan program utiliti kepada pekerja dan kakitangan penyelenggaraan IT yang secara khusus memerlukan mereka menjalankan peranan kerja mereka. b. Pastikan semua program utiliti dikenal pasti, disahkan dan dibenarkan selaras dengan keperluan perniagaan, dan pihak pengurusan dapat memperoleh pandangan atas bawah penggunaannya pada bila-bila masa. c. Kenal pasti semua kakitangan yang menggunakan program utiliti, sama ada sebagai sebahagian daripada tugas harian mereka, atau secara ad-hoc. d. Laksanakan kawalan kebenaran yang mencukupi untuk mana-mana pekerja yang perlu menggunakan program utiliti, sama ada sebagai sebahagian daripada tugas harian mereka atau secara ad-hoc. e. Menghalang penggunaan program utiliti pada mana-mana sistem yang dianggap perlu oleh organisasi untuk mengasingkan tugas. f. Semak semula penggunaan program utiliti secara berkala dan sama ada alih keluar atau lumpuhkan sebarang program sepertiyang diperlukan oleh organisasi. g. Program utiliti partition berbeza daripada aplikasi standard yangdigunakan oleh perniagaan secara tetap, termasuk trafik rangkaian. h. Hadkan ketersediaan program utiliti, dan gunakannya untuk tujuan nyata sahaja. i. Log penggunaan program utiliti, termasuk cap masa dan pengguna yang dibenarkan.	ICTSO, Pentadbir Teknikal, Pentadbir Rangkaian

8.19 PEMASANGAN PERISIAN PADA SISTEM OPERASI (*INSTALLATION OF SOFTWARE ON OPERATIONAL SYSTEMS)*	**PERANAN**
1. Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem operasi. Langkah-langkah yang perlu dipatuhi setelah mendapat kelulusan pegawai yang diberi kuasa melulus adalah seperti yang berikut: a. Strategi *rollback* perlu dilaksanakan sebelum sebarang perubahan ke atas konfigurasi, sistem dan perisian; b. Aplikasi dan sistem operasi hanya boleh digunakan setelah ujian terperinci dilaksanakan dan diperaku berjaya; dan c. Setiap konfigurasi ke atas sistem dan perisian perlu dikawal dan didokumentasikan dengan teratur.	Pentadbir Sistem Aplikasi
2. Peraturan yang mengawal pemasangan perisian oleh pengguna hendaklah disediakan dan dilaksanakan. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Hanya perisian yang diperaku sahaja dibenarkan bagi kegunaan warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yangmempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang. b. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang- undangbertulis yang berkuat kuasa; dan c. Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya.	Pentadbir SistemAplikasi, Warga Pejabat SUK Pahang, pembekal, pakar runding dan pihak yang mempunyai urusan dengan perkhidmatan ICT Pejabat SUK Pahang
8.20 KESELAMATAN RANGKAIAN (*NETWORKS* SECURITY)	**PERANAN**
Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman. Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; b. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; c. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d. Semua peralatan mestilah melalui proses *Factory Acceptance*	ICTSO, Pentadbir Rangkaian

Check (FAC) semasa pemasangan dan konfigurasi; e. Firewall hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir Rangkaian; f. Semua trafik keluar dan masuk dalam rangkaian Pejabat SUK Pahang hendaklah melalui firewall di bawah kawalan Pejabat SUK Pahang; g. Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; h. Memasang perisian *Intrusion Prevention System* (IPS) atau *Web Application Firewall* (WAF) mengikut kesesuaian bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat di dalam rangkaian Pejabat SUK Pahang; i. Memasang *Web Content Filtering* untuk menyekat aktiviti *Web Surfing* yang dilarang semasa waktu kerja; j. Sebarang penyambungan rangkaian yang bukan di bawah kawalan Pejabat SUK Pahang adalah tidak dibenarkan; k. Semua pengguna hanya dibenarkan menggunakan rangkaian Pejabat SUK Pahang sahaja dan penggunaan rangkaian lain seperti UNIFI perlu mendapatkan kebenaran atas sebab tertentu dan penggunaannya perlulah di bawah seliaan serta pemantauan ketua bahagian/unit masing-masing; l. Sebarang penggunaan rangkaian komunikasi daripada agensi lain (contoh: EGNet, NRENet) perlulah mendapat khidmat nasihat daripada pentadbir rangkaian terlebih dahulu dan pelaksanaan secara berpusat perlulah menjadi keutamaan; m. Kemudahan rangkaian tanpa wayar (*wireless*) perlu dipantau dan dipastikan kawalan keselamatan serta dikawal penggunaannya; n. Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Assurance* (SLA) yang telah ditetapkan; o. Menempatkan atau memasang antara muka (*interfaces*) yang bersesuaian di antara rangkaian Pejabat SUK Pahang, rangkaian agensi lain dan rangkaian awam; p. Mewujudkan dan menguatkuasakan mekanisme untukpengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya;	ICTSO, Pentadbir Rangkaian

q. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT yang dibenarkan sahaja; r. Mengawal capaian fizikal dan logikal ke atas kemudahan port diagnostik dan konfigurasi jarak jauh; s. Mengawal sambungan ke rangkaian khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan rangkaian Pejabat SUK Pahang; dan t. Mewujud dan melaksana kawalan pengalihan laluan (*routing control*) bagi memastikan pematuhan terhadap peraturan Pejabat SUK Pahang.	ICTSO, Pentadbir Rangkaian
8.21 KESELAMATAN PERKHIDMATAN RANGKAIAN (*SECURITY OF NETWORK SERVICES)*	**PERANAN**
Pengurusan bagi semua perkhidmatan rangkaian (*inhouse atau outsource*) yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenal pasti dan dimasukkan di dalam perjanjian perkhidmatan rangkaian.	ICTSO, Pentadbir Rangkaian, Pembekal
8.22 PENGASINGAN RANGKAIAN (*SEGREGATION OF NETWORKS*)	**PERANAN**
Pengasingan dalam rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian Pejabat SUK Pahang.	ICTSO, Pentadbir Rangkaian
8.23 PENAPISAN LAMAN WEB (*WEB FILTERING*)	**PERANAN**
Organisasi harus mewujudkan dan melaksanakan kawalan yang diperlukan untuk menghalang pekerja daripada mengakses laman web luaran yang mungkin mengandungi virus, bahan yang tidak selamat, data atau jenis maklumat haram yang lain dengan: a. Laman web dengan fungsi muat naik maklumat. Akses hendaklah tertakluk kepada kebenaran dan hanya boleh diberikan atas sebab yang sah mengikut Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 atau pekeliling-pekeliling semasa. b. Laman web yang diketahui atau disyaki mengandungi bahan berniat jahat, seperti laman web dengan kandungan perisian yang tidak selamat. c. Pelayan perintah dan kawalan.	ICTSO, Pentadbir Rangkaian, Pentadbir Teknikal

d. Laman web berniat jahat yang diperoleh daripada *scammer*. e. Laman web yang mengedarkan kandungan dan bahan yang menyalahi undang-undang.	ICTSO, Pentadbir Rangkaian, Pentadbir Teknikal
8.24 PENGGUNAAN KRIPTOGRAFI (*USE OF CRYPTOGRAPHY*)	**PERANAN**
1. Kriptografi merangkumi kaedah-kaedah seperti yang berikut: a. Enkripsi - Sistem aplikasi yang melibatkan maklumat terperingkat hendaklah dibuat enkripsi (*encryption*). b. Tandatangan Digital - Maklumat terperingkat yang perlu diproses dan dihantar secara elektronik hendaklah menggunakan tandatangan digital mengikut keperluan pelaksanaan. 2. Pengurusan ke atas Pengurusan Infrastruktur Kunci Awam *(Public Key Infrastructure)* PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	ICTSO, Pentadbir Rangkaian, Pentadbir Teknikal, Warga Pejabat SUK Pahang
8.25 KITARAN HAYAT PEMBANGUNAN SELAMAT (*SECURE DEVELOPMENT LIFE CYCLE)*	**PERANAN**
Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan untuk pembangunan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a. Keselamatan persekitaran pembangunan; b. Keselamatan pangkalan data; c. Keperluan keselamatan dalam fasa reka bentuk; d. Keperluan *check point* keselamatan dalam carta perbatuan projek; e. Keperluan pengetahuan ke atas keselamatan aplikasi; f. Keselamatan dalam kawalan versi; dan g. Bagi pembangunan secara penyumberluaran (*outsource*), pembekal yang dilantik berkebolehan untuk mengenal pasti dan menambah baik kelemahan dalam pembangunan sistem.	ICTSO, Pentadbir Sistem Aplikasi

8.26 KEPERLUAN KESELAMATAN APLIKASI (*APPLICATION SECURITY REQUIREMENTS)*	**PERANAN**
1. Perkara yang perlu dipertimbangkan adalah seperti berikut: a. Semua perkhidmatan sumber luaran hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Perkhidmatan sumber luaran adalah perkhidmatan yang disediakan oleh organisasi luar untuk menyokong operasi Pejabat SUK Pahang. Contoh perkhidmatan sumber luaran ialah: i. Perisian sebagai satu perkhidmatan; ii. platform sebagai satu perkhidmatan; iii. Infrastruktur sebagai satu perkhidmatan; iv. Storan pengkomputeran awan; dan v. Pemantauan keselamatan. b. Saluran komunikasi dan aliran data kepada perkhidmatan ini hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala; c. Tahap kerahsiaan bagi mengenai pasti identiti masing-masing, misalnya melalui pengesahan (*authentication*); d. proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi; e. Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan aplikasi dan perkhidmatan ICT; dan f. Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak.	Pentadbir Sistem Aplikasi, ICTSO, Pengurus ICT
2. Maklumat yang terlibat dalam urusan perkhidmatan aplikasi hendaklah dilindungi bagi mengelakkan penghantaran tidak sempurna, salah destinasi, pindaan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan, penduaan atau ulang tayang mesej yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti yang berikut: a. Penggunaan tandatangan elektronik oleh setiap pihak yangterlibat dalam transaksi; b. Memastikan semua aspek transaksi dipatuhi: i. maklumat pengesahan pengguna adalah sah digunakan dan telah disahkan; ii. mengekalkan kerahsiaan maklumat; iii. mengekalkan privasi pihak yang terlibat; dan	Pentadbir Sistem Aplikasi

iv. protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi. c. Pihak yang mengeluarkan tandatangan digital ialah yang dilantik oleh Kerajaan.	Pentadbir Sistem Aplikasi
8.27 PRINSIP SENIBINA DAN KEJURUTERAAN SISTEM SELAMAT *(SECURE SYSTEM ARCHITECTURES AND ENGINEERING PRINCIPLES)*	**PERANAN**
Prinsip bagi sistem keselamatan kejuruteraan hendaklah disediakan, didokumenkan, diselenggara dan digunakan untuk apa-apa usaha pelaksanaan sistem maklumat. Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari semasa ke semasa dalam semua peringkat pembangunan sistem bagi memastikan keberkesanan kepada keselamatan maklumat berpandukan kepada Garis Panduan dan Pelaksanaan *Independent Verification and Validation (IV&V)* sektor awam yang terkini.	Pentadbir Sistem Aplikasi
8.28 PENGEKODAN SELAMAT (*SECURE CODING*)	**PERANAN**
Amalan dan prosedur pengekodan yang selamat hendaklah mengambil kira perkara berikut untuk proses pengekodan: a. Prinsip pengekodan perisian yang selamat harus disesuaikan dengan setiap bahasa pengaturcaraan dan teknik yang digunakan. b. Penggunaan teknik dan kaedah *secure coding* seperti pembangunan yang hendak dilakukan hendaklah dibuat pengujian dan pemasangan pasangan (*pair programming*). c. Penggunaan kaedah pengaturcaraan yang berstruktur. d. Dokumentasi kod yang betul dan penyingkiran kecacatan kod. e. Larangan ke atas penggunaan kaedah pengekodan perisian yang tidak selamat seperti sampel kod yang tidak diluluskanatau kata laluan berkod keras (*hard coded*). f. Kod yang digunakan hendaklah sentiasa dikemaskini mengikut keadaan keselamatan semasa.	Pentadbir Sistem Aplikasi

8.29 PENGUJIAN KESELAMATAN DALAM PEMBANGUNAN DAN PENERIMAAN (*SECURITY TESTING IN DEVELOPMENT AND ACCEPTANCE*)	**PERANAN**
1. Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan sistem. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat; b. Membuat semakan pengesahan di dalam aplikasi untuk mengenai pasti kesilapan maklumat; dan c. Menjalankan proses semak dan pengesahan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan.	ICTSO, Pentadbir Sistem Aplikasi
2. Program pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk sistem maklumat yang baharu, yang ditambah baik dan versi baharu. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat; b. Pengujian penerimaan sistem hendaklah merangkumi Keperluan Keselamatan Sistem Maklumat dan kepatuhan kepada Polisi Pembangunan Selamat; c. penerimaan pengujian semua sistem baharu dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem digunapakai; dan d. pengujian semua sistem baharu boleh menggunakan alat imbasan automatik yang digunakan untuk ujian imbasan kerentanan *(vulnerability scanner*).	ICTSO, PentadbirSistem Aplikasi, Pengguna
8.30 PEMBANGUNAN OLEH PIHAK LUAR (*OUTSOURCED DEVELOPMENT)*	**PERANAN**
Pembangunan aplikasi secara *outsource* perlu diselia dan dipantau oleh pegawai yang dipertanggungjawabkan. Kod sumber (*source code*) bagi semua aplikasi dan perisian adalah menjadi hak milik Pejabat SUK Pahang. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Perkiraan perlesenan, kod sumber ialah HAK MILIK Pejabat SUK Pahang dan harta intelek sistem yang berkaitan dengan pembangunan perisian aplikasi secara *outsource;* b. Bagi semua perkhidmatan sumber luaran, perisian sebagai satu	ICTSO, Pentadbir Sistem Aplikasi

perkhidmatan yang mengendalikan Maklumat Rahsia Rasmi, spesifikasi perolehan dan kontrak komersial hendaklah memasukkan keperluan mandatori "Pembekal **hendaklah membenar Kerajaan hak** mencapai kod sumber dan melaksanakan pengolahan risiko"; c. Keperluan kontrak untuk reka bentuk selamat, pengekodan dan pengujian pembangunan sistem yang dijalankan oleh pihak luar mengikut amalan terbaik; d. Penerimaan pengujian berdasarkan kepada kualiti dan ketepatan serahan sistem; e. Mengguna pakai prinsip dan tatacara *escrow* (sekiranya perlu*)*; dan f. Mematuhi keberkesanan kawalan dan undang-undang dalam melaksanakan pengesahan pengujian.	ICTSO, Pentadbir Sistem Aplikasi
8.31 PENGASINGAN PERSEKITARAN PEMBANGUNAN , PENGUJIAN DAN OPERASI (*SEPARATION OF DEVELOPMENT, TEST AND PRODUCTION ENVIRONMENT*)	**PERANAN**
Organisasi hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem. Pejabat SUK Pahang perlu menilai risiko yang berkaitan semasa pembangunan sistem dan membangunkan persekitaran selamat dengan mengambil kira: a. Sensitiviti data yang akan diproses, disimpan dan dihantar oleh sistem; b. Terpakai kepada keperluan undang-undang dan peraturan dalaman dan luaran; c. Keperluan dalam pengasingan di antara pelbagai persekitaran pembangunan sistem; d. Kawalan pemindahan data dari atau ke persekitaran pembangunan sistem; e. Pegawai yang bekerja di dalam persekitaran pembangunan sistem ialah yang boleh dipercayai; dan f. Kawalan ke atas capaian kepada persekitaran pembangunan sistem.	Pentadbir Sistem Aplikasi

8.32 PENGURUSAN PERUBAHAN (*CHANGE MANAGEMENT*)	PERANAN
1. Perubahan pada sistem dalam kitar hayat pembangunan hendaklah dikawal dengan menggunakan prosedur kawalan perubahan yang telah ditetapkan. Perubahan ke atas sistem hendaklah dikawal. Perkara-perkarayang perlu dipatuhi adalah seperti berikut : a. perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; b. aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor; c. Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; d. Keperluan dan kesesuaian perubahan terhadap sistem pengoperasian dan perisian sokongan perlu dikaji terlebih dahulu. e. Sebarang perubahan sistem pengoperasian dan perisian sokongan perlu diuji dahulu di dalam *development server* sebelum dipasang di dalam server sebenar. f. Akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan g. Menghalang sebarang peluang untuk membocorkan maklumat.	Pengurus ICT, Pentadbir Sistem Aplikasi
2. Apabila platform operasi berubah, aplikasi penting perniagaan hendaklah dikaji semula dan diuji bagi memastikan tiada kesan buruk ke atas operasi atau keselamatan organisasi. Perkara yangperlu dipatuhi adalah seperti yang berikut: a. Pengujian ke atas sistem adalah perlu untuk memastikan sistem tidakterjejas apabila berlaku perubahan platform; b. Perubahan platform dimaklumkan kepada pihak yang terlibat bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan;dan c. Memastikan perubahan yang sesuai dibuat kepada PKP Pejabat SUK Pahang dan Pelan Pemulihan Bencana Sistem yang berkaitan berdasarkan Pelan Pengurusan Keselamatan	Pentadbir Sistem Aplikasi

Maklumat (ISMP) sistem tersebut. 3. Pengubahsuaian ke atas pakej perisian adalah tidak digalakkan, ia terhad kepada perubahan yang perlu dan semua perubahan hendaklah dikawal dengan ketat.	Pengurus ICT,Pentadbir Sistem Aplikasi
8.33 MAKLUMAT UJIAN (*TEST INFORMATION*)	**PERANAN**
Data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal. Perkara yang perlu dipatuhi adalah seperti yang berikut: a. Sebarang prosedur kawalan persekitaran sebenar hendaklah juga dilaksanakan dalam persekitaran pengujian; b. Personel yang mempunyai hak capaian persekitaran sebenar sahaja dibenarkan untuk menyalin data sebenar ke persekitaran pengujian; c. Data sebenar yang disalin ke persekitaran pengujian hendaklah dipadam sebaik sahaja pengujian selesai; dan d. Mengaktifkan log audit bagi merekodkan sebarang penyalinan dan penggunaan data sebenar.	ICTSO, Pentadbir Sistem Aplikasi
8.34 PERLINDUNGAN SISTEM MAKLUMAT SEMASA PENGUJIAN AUDIT (*PROTECTION OF INFORMATION SYSTEMS DURING AUDIT TESTING*)	**PERANAN**
Keperluan dan aktiviti audit yang melibatkan pengujian sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas proses kelancaran sistem.	ICTSO, Pentadbir Sistem Aplikasi

GLOSARI

Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, *optical disk, flash disk, CDROM, thumb drive* untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	LebarJalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam angka masa yang ditetapkan.
CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supayatidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*), penipuan (*hoaxes*).
CSIRT Pejabat SUK Pahang	*Computer Security Incident Response Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT Pejabat SUK Pahang.
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.

Hub	Hab (hub) merupakan peranti yang menghubungkan dua atau lebih stesenKerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (broadcast) data yang diterima daripada sesuatu port kepada semua port yang lain.
ICT	Information and Communication Technology (Teknologi Maklumat dan Komunikasi)
ICTSO	ICT Security Officer Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian- rangkaian tersebut agar sentiasa berasingan.
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat host atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau malicious code. Contohnya: Network-based IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
Logout	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus,trojan horse, worm, spyware dan sebagainya.

MODEM	Modulator DEModulator Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaianInternet dibuat dari komputer.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi- fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakandalam jangka masa tertentu.
Server	Pelayan komputer
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/Collision Detection* (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaranyang berlaku.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif peribadi dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepadapengguna dalam masa yang sama ia diterima oleh penghantar.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

LAMPIRAN 1 : SURAT AKUAN PEMATUHAN POLISI KESELAMATAN SIBER PEJABAT SUK PAHANG

SURAT AKUAN PEMATUHAN POLISI KESELAMATAN SIBER PEJABAT SUK NEGERI PAHANG

SURAT AKUAN PEMATUHAN

POLISI KESELAMATAN SIBER PEJABAT SUK NEGERI PAHANG

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Bahagian / Unit / Syarikat : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Polisi Keselamatan Siber Pejabat SUK Negeri Pahang; dan
2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tanda tangan : .....

Tarikh : .....

Rujukan:

Sila layari POLISI KESELAMATAN SIBER PEJABAT SUK NEGERI PAHANG di http://www.pahang.gov.my/

LAMPIRAN 2 : SURAT PERAKUAN PEMATUHAN AKTA RAHSIA RASMI 1972 [AKTA 88] DAN POLISI KESELAMATAN SIBER PEJABAT SUK PAHANG

PERAKUAN UNTUK DITANDATANGANI BERKENAAN DENGAN AKTA RAHSIARASMI 1972 [AKTA 88] DAN POLISI KESELAMATAN SIBER PEJABAT SUK PAHANG

NAMA PROJEK :……

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 [Akta 88] dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah, sesuatu benda rahsia, tidak menjaga dengan cara yang berpatutan sesuatu rahsia atau apa-apa tingkah laku yang membahayakan keselamatan atau rahsia sesuatu benda rahsia adalah menjadi sesuatu kesalahan di bawah Akta tersebut, yang boleh dihukum maksimum penjara seumur hidup.

Saya faham bahawa segala maklumat rasmi yang saya perolehi adalah milik Pejabat SUK Pahang dan tidak akan membocorkan, menyiarkan atau menyampaikan, sama ada secara lisan atau dengan bertulisan atau secara media elektronik, kepada sesiapa jua dalam apa-apa bentuk, kecuali pada masa menjalankan kewajipan-kewajipan rasmi saya, sama ada dalam masa atau selepas perkhidmatan saya dengan mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapatkan kebenaran bertulis pihak berkuasa yang berkenaan.

Saya juga turut tertakluk di bawah Polisi Keselamatan Siber Pejabat SUK Pahang terkini berkenaan Perkara: Menangani Keselamatan Maklumat Dalam Perjanjian Pembekal. Selain itu, saya juga telah membaca dan faham serta akan mematuhi polisi lain di dalam Polisi Keselamatan Siber Pejabat SUK Pahang yang berhubungkait dengan urusan ini.

Saya juga dengan ini mewakili ….....
mengakui bahawa semua maklumat yang dinyatakan seperti di **Lampiran A** adalah terlibat secara langsung bagi sebarang urusan yang memerlukan pematuhan akta dan Polisi Keselamatan Siber Pejabat SUK Pahang seperti semua keterangan perenggan di atas. Oleh itu, sesiapa yang tiada dalam senarai **Lampiran A** tersebut tidak dibenarkan terlibat secara langsung bagi sebarang urusan melibatkan peruntukan Akta Rahsia Rasmi 1972 [Akta 88].

*** Sila lengkapkan dengan tulisan HURUF BESAR**

Tandatangan:……..	**Disaksikan oleh :……**
Nama :……	**Nama :……..**
No. Kad Pengenalan :……	**No. Kad Pengenalan :……**
Jawatan :……	**Jawatan :……**
Jabatan/Syarikat :……	**Jabatan/Syarikat :……**
Tarikh :……..	**Tarikh :……**
Alamat Jabatan/Syarikat :	**Cop Jabatan/Syarikat :**

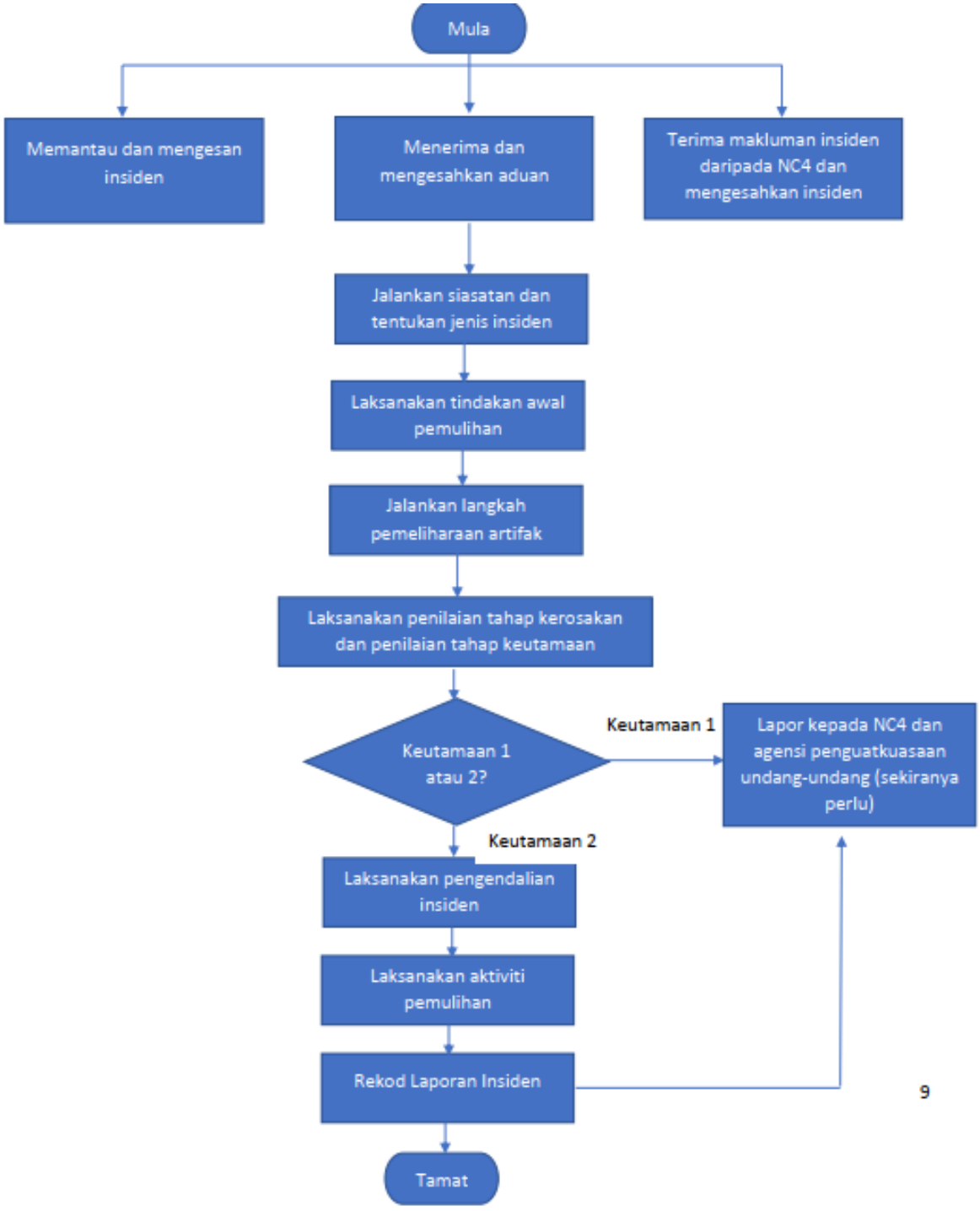
LAMPIRAN A

SENARAI KAKITANGAN JABATAN / SYARIKAT YANG TERLIBAT DALAM URUSAN ANTARA JABATAN / SYARIKAT ..... DENGAN PEJABAT SUK PAHANG .

*** Sila lengkapkan dengan tulisan HURUF BESAR**

Bil	Nama & Jabatan	Jawatan Syarikat	No. K/P

LAMPIRAN 3 : PROSES KERJA PELAPORAN INSIDEN KESELAMATAN SIBER PEJABAT SUK PAHANG



LAMPIRAN 4 : SENARAI PERUNDANGAN DAN PERATURAN

1. Arahan Keselamatan (Semakan dan Pindaan 2017);
2. Akta Rahsia Rasmi 1972 [Akta 88];
3. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
4. Surat Arahan Ketua Pengarah MAMPU - Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 Dalam Sektor Awam bertarikh 24 Nov 2010
5. Surat Arahan Ketua Pengarah MAMPU - Panduan Keperluan dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC27001:2007 dalam Sektor Awam bertarikh 24 Nov 2010
6. Surat Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian Government Computer Emergency Response Team (GCERT) oleh NACSA bertarikh 28 Januari 2019
7. Surat Pemakluman Pengurusan Maklumat Pegawai Keselamatan ICT (ICTSO) Sektor Awam bertarikh 28 Februari 2019
8. Surat Pemakluman Kaedah Pelaksanaan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 6 April 2022
9. Pekeliling Am Bilangan 4 Tahun 2022 - Pengurusan dan Pengendalian Insiden Keselamatan Siber Sektor Awam bertarikh 1 Ogos 2022
10. Surat Pekeliling Am Bilangan 3 Tahun 2024 - Garis Panduan Pengurusan Risiko Keselamatan Maklumat Sektor Awam bertarikh 21 Mac 2024
11. Surat Pekeliling Am Bilangan 4 Tahun 2024 - Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam bertarikh 21 Mac 2024
12. Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) V1.0 MAMPU (April 2016)
13. Akta Tandatangan Digital 1997 [Akta 562];
14. Akta Jenayah Komputer 1997 [Akta 563];
15. Perintah-perintah Am;
16. Akta Hak Cipta (Pindaan) 2022;
17. Akta Komunikasi dan Multimedia 1998 [Akta 588];
18. Arahan Perbendaharaan (Pindaan 2023);
19. 1PP/AM1.1 Pekeliling Perbendaharaan Malaysia – Pengurusan Aset Kerajaan
20. 1PP/PK2 Pekeliling Perbendaharaan Malaysia – Kaedah Perolehan Kerajaan
21. Akta Keselamatan Siber 2024 dan Peraturan-peraturan [Akta 854]
22. Surat Pekeliling YB SUK PAHANG : Bil 05 Tahun 2008 : Arahan Keselamatan Penggunaan Komputer Riba Di Jabatan-jabatan Kerajaan Negeri Pejabat SUK Pahang
23. Surat Arahan YB SUK PAHANG (13 Jan 2011) : Larangan Penggunaan Perisian Tidak Berlesen di Komputer Milik Kerajaan
24. Surat Arahan YB SUK PAHANG (13 Jun 2011) : Pendaftaran Aset Milik Persendirian dan Sumbangan
25. Surat Arahan CIO (21 Apr 2011) : Perkongsian Pencetak di Pejabat SUK Negeri Pejabat SUK Pahang dan Jabatan Negeri Pejabat SUK Pahang.
26. Surat Arahan (28 Mac 2016) : Pelaksanaan Penyelenggaraan Berjadual Bagi Aset ICT Dan Peraturan Kepada Pemilik Aset ICT Pejabat SUK Pahang